EXPLORING SOLUTIONS TO INTERNET VOTING IN GOVERNMENT ELECTIONS IN THE UK

By

Cheylea Hopkinson

A DISSERTATION

Submitted to

The University of Liverpool

in partial fulfilment of the requirements
for the degree of

MASTER OF SCIENCE COMPUTER SCIENCE

15/01/2024

DECLARATION

I hereby certify that this dissertation constitutes my own product, that where the language of others is set forth, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions, or writings of another.

I declare that the dissertation describes original work that has not previously been presented for the award of any other degree of any institution.

Signed,

Cheylea Hopkinson

Student, Supervisors and Classes:

Student name:	Cheylea Hopkinson
Student ID number:	
DI name:	Kathleen Kelm
DA name:	Andrea Corradini

EXPLORING SOLUTIONS TO INTERNET VOTING IN GOVERNMENT ELECTIONS IN THE UK

A DISSERTATION

Submitted to

The University of Liverpool

in partial fulfilment of the requirements
for the degree of

MASTER OF SCIENCE COMPUTER SCIENCE

15/01/2024

ABSTRACT

EXPLORING SOLUTIONS TO INTERNET VOTING IN GOVERNMENT ELECTIONS IN THE UK

In a country of continuing digital development, why does the United Kingdom (UK) still vote using paper voting for government elections? There are many potential advantages of internet e-voting: it is convenient, fast and would potentially cost the government less (Mackenzie, 2019). However, many concerns remain as to whether a system can be secure and trustworthy. “Could the system be hacked?” “How do I know my vote will be counted?” “Will my data be safe?” Through literature appraisal, this project develops a list of required criteria for a safe vote, which, as it stands, there is no existing end-to-end solution that satisfies all criteria.

This project explores internet electronic voting (e-voting) and whether a proposed e-voting tool could be private, secure, and trustworthy. The tool includes biometric identification, blockchain voting and secret word self-verification for participants to confirm their vote is accurate. Between October and December 2023, a prototype was created, tested, and surveyed by the UK public to find its feasibility and effectiveness to satisfy the criteria for voting. The evaluation has three main themes: can e-voting be both accurate and private, does e-voting mean a less secure vote, and can both the governing body and public have two-way trust of the system.

The results find that there is potential to use blockchain as a technological solution to e-voting but there remains further development to finding a fully secure solution that is universally understood and trusted by people that may not be experts in this field. The prototype tool used is a step closer to what a system could look like in the future, but if the UK were to rollout such a system, it would need to have airtight processes sustaining trust in the system and mitigating where social doubt could be cast.

ACKNOWLEDGEMENTS

Firstly, thank my friends, acquaintances and even strangers for listening to me about my projects and studies, for being sounding boards for my trials and for keeping me smiling. Second, I would like to thank my university lecturers and work colleagues for all their input, time, and understanding while working through this project and degree. I would like to thank Amy, who kept my visualisation formatting in check and beyond. I would also like to thank my advisor, Andrea, for the reassurance and guidance. Thirdly, I thank my family for their help, support, and encouragement. Thank you to my Dad, who took a constant interest in this degree and challenged the way I think; my Mum, for being a continual stream of positivity; and my Auntie Valerie, who never stopped chasing me to apply and do a master's degree in the first place (albeit not in the subject she was expecting!).

I want to thank three people for everything they have done for me while working on this project and degree.

To Wayne, thank you for encouraging me to go into computer science, inspiring me with your high standards and passion for problem-solving, and being there at the latest hours to send me in the right direction.

To Alexandra, thank you for getting me through the most formidable challenges not only on this course but personally as well. It is not often you meet someone like you, and I'm unsure if I would have continued and finished this degree without you.

And finally, to James, thank you for pushing me far out of my comfort zone and beyond what I even thought I could achieve. Thank you for wiping off tears, picking me up off the ground, and never letting me think I could not do it for a second. Thank you for the energy, love, and time. Thank you for everything.

TABLE OF CONTENTS

LIST OF TABLES

Page

LIST OF FIGURES

Page

Chapter 1. INTRODUCTION

1.1 Chapter Introduction

Through its conception and modernisation, the United Kingdom's (UK) democratic elections have grown and evolved with it. From the elite lords and ladies of the Victorian era to citizens and denizens of all backgrounds today (Norfolk Archives, 2022). From the vote counting timeframes that spanned a month (Durkin and White, 2007) to the recent overnight races to count council ballots (BBC News, 2019). But has that evolution stagnated for the elective system methodology, and what role could modern technology play in its progress?

Voting in UK elections involves marking a paper ballot in-person at a polling station or by post. These solutions require vast amounts of physical resources, planning, and human labour to realise. For example, the 2015 general election cost £114.73 million to carry out, with printing costs and thousands of staff collecting and counting votes (HM Government, 2018). While general elections occur at least once within a five-year period, more regular elections, such as the local council or police commissioner elections, contribute even further to these costs (GOV.UK, n.d.). Furthermore, the cost is just one of the many disadvantages of paper voting. Others include transparency for the voter to know their vote is counted as expected and the potential inconvenience of long waiting times (Smys, Balas and Palanisamy, 2022, pp.89–105). In the age of digitisation and the internet - can we do better?

Electronic voting (e-voting) is the concept of completing an election vote through the assistance of technology. There are two types of e-voting: in-person voting machines and votes cast remotely using the internet (Faruk et al., 2022). This research will focus on internet e-voting, and any further reference to e-voting in this paper will refer to internet e-voting unless otherwise distinguished. From a purely conceptual perspective, one might consider that the model of internet e-voting is easily 'solvable'. In that, it is possible to create an application where a voter can cast a vote from a device in their own home that can be stored remotely using the internet, and subsequently counted. However, in reality, this is insufficient to guarantee a voting system's accuracy. It remains possible for citizens to lie about an identity when voting, or for votes to be intercepted, or even amended by bad actors (Birmingham City Council, 2023). Potential nefarious activity casts doubt on whether the government could implement such a system to replace in-person voting.

This research explores the advantages and disadvantages of internet e-voting and whether a working prototype can overcome these issues so roll-out of this technology could be possible in the UK.

1.2 Problem Statement

Many citizens might hold the view that there is no problem with democratic elections, and traditional paper and post methods are the best. Indeed, the UK's resistance to changes can be clearly evidenced in the results of the 2011 United Kingdom Alternative Vote referendum, where the progressive Alternative Vote method was rejected by a healthy margin (BBC News, 2011). However, it cannot be denied that internet e-voting has the potential for a swathe of benefits, including much lower expenditure to run elections (ElectionBuddy, 2022), higher levels of voter independence (especially for disabled voters or those with mobility issues) (Engage, 2018) and verification features offers two-way transparency.

Anonymity in voting is essential to ensure people are not discriminated against for their political views or coerced into voting in a certain way. Within the UK, the government recommends that local authorities stop people from taking photos of their ballot paper to preserve ballot secrecy (Electoral Commission, 2023a). Political opinions are highly divisive, and protecting voters from negative consequences depending on how they vote is essential to ensure it is fair. Preserving this secrecy ensures that how someone votes cannot be evidenced and avoids the possibility of a third party influencing the person to do so, removing the possibility of discrimination (UK Parliament, 2019). Moving voting into people's homes may mean people can vote without assistance, but it removes the ability to regulate unwanted coercion attempts from others. As a result, maintaining anonymity is an imperative part of an internet e-voting system to keep voters safe from adverse effects when voting.

Unlike paper voting, where ballots need printing, staff to man poll stations and people to count each vote physically, electronic voting is relatively instant, and results can be automatically tallied by the computer system, eliminating much of the manual processes (ElectionBuddy, 2022). However, the security considerations of electronic voting are largely different to those of paper voting. Suppose a bad actor could access a database of votes and alter them. In that case, this impact scales up much more than paper voting (Park et al., 2021), which would involve convincing many vote counters to change votes to make a significant impact.

Disabled voters have many barriers when it comes to voting including “physical, psychological and information barriers when voting at a polling station” (Electoral Commission, 2023b). With internet e-voting, voters can vote from the comfort of their homes, which can be more convenient and accessible for those with mobility issues or other disabilities. It also provides independence to many, who would not require extra assistance when voting if able to do so through their laptop or tablet, which could arguably help reduce coercion (Engage, 2018).

Changes to the voting system can be taken poorly by UK citizens. The local government elections on 4th May 2023 were the first-time voters were required to show photo identification to vote in person (Uberoi and Johnston, 2023). The government introduced this requirement based on recommendations from the Electoral Commission and to minimise those lying about their identity to vote (Johnson, 2023). This change brought about mixed responses from the UK public and was not without controversy (Moorhouse, 2023), with poll clerks receiving abuse on the day (Sefton Council, 2023). One argument against this change by the public was that the government implemented it to suppress voters less likely to have certain types of ID (Toynbee, 2022). For anyone with a valid form of ID, free Voter Authority Certificates are available in England, Scotland, and Wales and Electoral Identity Cards in Northern Ireland. Although this seems like a straightforward answer to the problem for anyone who wants to vote, the inconvenience barrier alone leads to mistrust of the intentions behind the system (Toynbee, 2022) which can lead to adverse reactions from the UK public. Implementing a more extensive change like internet e-voting would require extensive trust and should not introduce more barriers to voting.

The advantages of progressing e-voting research are clear, but the consequences of not doing it right could violate the values of democracy. With all this, this research will ask three questions:

1. Can an internet e-voting system identification check be remote whilst ensuring accuracy and voter anonymity?

2. Would an internet e-voting system compromise the security of the vote casting?

3. Can an internet e-voting system provide two-way transparency between voters and the governing body?

1.3 Project Aims and Objectives

This project will develop a new internet e-voting tool using a new framework that attempts to address some of the concerns with existing e-voting systems, in the context of UK government elections.

First, a base of knowledge must be established, via a literature review, to explore:

- further possible specifications a trusted system would need to incorporate
- a set list of criteria all stakeholders would expect an e-voting solution to include
- a design and concept, grounded on successful prototypes or early solutions

Once this base of knowledge is established, an IT artefact will be designed taking into consideration identification, security and transparency and the issues that arise when trying to meet these criteria. With this as a foundation, a secure e-voting application accessible through the internet will be developed and evaluated using designed tests. The artefact must hold an original element to the design to foster results for a new approach and how it may differently address challenges. These aims will plot a course to an end-to-end verifiable solution by surveying public reaction to a new theoretical tool and exploring if they can understand and trust it.

1.4 Approach

One focus of this research will be examining a potential technological solution – Blockchain. Quintessentially, blockchain is a decentralised technology that creates records that external parties cannot change. When an application mines a new block and adds it to the chain, the chain is broadcast onto a network of multiple machines (Hayes, 2023). If a bad actor were to attempt to compromise one of the machines by inserting, changing, or deleting a block, it cannot be done without detection (Jafar, Aziz and Shukur, 2021). Many proposed frameworks for e-voting systems use blockchain. Faruk et al. (2022) present an explicit framework for eliminating voter fraud in their work relating to Biometric identification with blockchain. Zeng et al. (2021) use blockchain to create a self-tallying voting system. Both function as a conceptual model of a decentralised system that harnesses the benefits of blockchain.

To effectively assess any e-voting model, the public must be able to analyse the system themselves to foster trust (Jafar, Aziz and Shukur, 2021). Because of this, real UK participants must be asked for feedback and while doing so be given the best possible tools to enact this analysis.

This project will foster a mixed-method approach and analyse the effectiveness of the IT artefact in the following ways:

- **Qualitative analysis (Literature Review):** Conduct a literature review to understand the current UK attitude towards e-voting, the strengths and weaknesses of existing systems, and the disadvantages of paper voting. Various case studies within the literature review will examine examples of existing e-voting systems and their advantages, disadvantages, and lessons learned.

- **Mixed-method analysis of IT Artefact:** Testing the artefact on the effects of malicious interference and its trustworthiness afterwards. The artefact will undergo three tests to achieve this: voting simulation, back-end simulations including controlled hacks and a public survey.

The findings from the above will establish the current mindset around internet e-voting, whether the proposed tool works and if the public can trust it.

1.5 Outcome

For something like an election, changing and controlling how a country is governed is a powerful tool for anyone. The outcome of this research will determine if the finished IT artefact satisfies several aims to preserve the fairness of voting. For the IT artefact to succeed, it must show the potential to satisfy all the problem statement questions. And so, it will combine several features to achieve this, including an original approach to vote-verification by the voters themselves.

- **Identity checks are accurate and anonymous:** The artefact must be able to verify the identity of voters successfully and safely without risking their anonymity and privacy. The results of these identity checks need to be consistent and dependable, so any identification tests must give 100% accuracy for any positive ID matches, and positive matches that fail should be as minimised as possible.

- **Vote security is not compromised:** There must be no risk to the security of the vote. Functional tests will determine if it mitigates the risk of vote manipulation and must have no security gaps. Survey participants will need to respond positively to feeling their vote would be secure.

- **There is two-way transparency:** To introduce two-way transparency, participants must be satisfied that their vote (and all others) is cast in the way they intend. Survey participants must respond positively to the proposed vote-verification method to fully evaluate if this is the case.

- **It is trustworthy:** The artefact will contain information about blockchain, and the researcher will determine if a voter can understand how it works to the extent that they can assess the tool themselves to determine if they feel comfortable voting in this way. E-voting should not introduce more barriers to voting, which could foster mistrust (Toynbee, 2022), so the tool must be easy to use.

It is only through these specific outcomes that the artefact can be considered successful. This is due to how they directly relate to the preestablished project aims and problem statements.

1.6 Chapter Summary

Internet e-voting could change how we vote, but a base of research and knowledge must be available before nations fully commit to a complete end-to-end solution. This research intends to be a vital step in the evolution of e-voting and will help indicate the direction progress must take against a backdrop of shifting public opinions.

All democratic nations face the challenges of election expenditure, transparency, voter anonymity, and integrity. It is right that the technology we consider bleeding edge now is explored thoroughly and with potential integration, incorporated into traditionally conservative practices.

Before considering rollout in any country, however, we must analyse what has been done right so far, the hurdles others have faced, and liberally research peoples' preestablished views, on what can be a contentious subject.

Chapter 2. Background and Review of Literature

2.1 Chapter Introduction

To analyse the problem statement further, we must begin to look at the existing body of research for internet e-voting. Researchers and academics alike have previously explored e-voting through numerous research methods. In some cases, e-voting systems in government elections already exist, such as in countries like Estonia (Scytl, 2021). From this available research and lessons learned, this chapter aims to establish detailed requirements for e-voting tools, and gaps in the research that need further exploration. To do this, this chapter will summarise available studies and approaches to develop an in-depth list of criteria for the e-voting tool and theorise a new approach.

2.2 Research Background

If a person is eligible to vote in the UK, they must still register before a set deadline before poll day. The government provides data from these registrations and circulates them to the respective polling station, with a list of registered voters whose eligibility is checked first, followed by an identity check, before handing them their ballot paper (Johnston, 2021). Voters can then complete their vote by marking their ballot against the appropriate number of candidates for the election. It is also worth noting how voters have the democratic option to spoil or leave their ballot incomplete, where no official vote is counted, or it cannot legitimately be determined who the vote would be for (Fisher, 2019). These democratic options are considered essential functions of an election to some, so an effort should be made to include these in a design appropriate for UK use.

To determine the necessary criteria for a voting system, we first look at literature that sets the design standard for a good system. Hao et al. (2020) define a verifiable system as votes being recorded accurately with a voter being able to confirm their completed vote is for the candidate they intended to vote for, as well as an external observer being able to substantiate whether the vote counts are correct. Verifiable systems are good starting points for the tools' requirements, but the design must consider other potential criteria. Denis González et al. (2022) present criteria such as unchangeable, receipt-free, accessible, and storing votes in a decentralised way. They describe how voters should be content

that their vote will not change and can cast it easily despite any potential disability. Regarding receipt-freeness specifically, a voter is entitled to vote privately and, as such, needs to have their privacy protected when voting, not positioned where a third party could coerce them to show or change their vote.

Traditional paper voting is not verifiable, and therefore remains open to an element of risk of human error or even deliberate deception. As such, it remains possible that eligibility or identity checks can be missed or performed poorly, whereas online identification systems may have better security (Davies, 2023). However, with the number of human participants involved in the countrywide vote, scaling up this vote manipulation is more challenging than with e-voting systems (Jafar, Aziz and Shukur, 2021).

2.3 Literature Review

Risks and Opportunities of Blockchain-Base on E-Voting Systems

Abuidris, Y., Hassan, A., Hadabi, A. and Elfadul, I. (2019). *Risks and Opportunities of Blockchain Based on E-Voting Systems.* IEEE Xplore. doi:https://doi.org/10.1109/ICCWAMTIP47768.2019.9067529.

This paper summarises the advantages and disadvantages of blockchain and caters to audiences of users and developers alike. As it describes, blockchain has the potential to be useful for e-voting systems due to how stored blockchain data could effectively prevent unauthorised alteration. The features of blockchain mean that, if used in a voting system, it would be difficult to change the values of votes once cast and committed. However, although blockchain introduces advantages and solutions to security, he details how not all scenarios are solved and how introducing a system into democracy may have adverse results. The paper also identifies disadvantages, including vulnerabilities such as not being tested on a full scale, limited scope to prevent vote-buying, and the difficult balance between voter eligibility and anonymity. Vote verification is essential in a blockchain model to ensure voters can trust their vote has been successfully committed to the immutable blockchain. This verification should highlight whether a vote was intercepted or changed in the interim. However, privacy in the verification is also vital. The paper states that “Once it is on the blockchain, we want the person to see that is their vote, but we do not want anyone else to see what is going on because it does not help to make sure the voting is reasonable.” (Abuidris et al., 2019, p.367).

It successfully captures the general problems that arise when implementing e-voting with blockchain. It concludes that this technology is still early and would demand far more research to develop something entirely successful.

Internet voting in Estonia 2005–2019: Evidence from eleven elections

Ehin, P., Solvak, M., Willemson, J. and Vinkel, P. (2022). Internet voting in Estonia 2005–2019: Evidence from eleven elections. Government Information Quarterly, 39(4), p.101718. doi:https://doi.org/10.1016/j.giq.2022.101718.

Estonia is one of the few countries to use internet voting, which began in 2005. This paper describes the technical specifications for their voting and analyses the demographics and survey results to assess the effectiveness of internet voting.

Their current e-voting system has been in use since 2017. The voting record is encrypted and signed with the voter's "eID" (Ehin et al., 2022, p.5) when a vote is cast. This is sent to a registration service that returns a timestamp to confirm that the vote has been committed. The voter can then verify their vote with a reference number to check the value of the vote and the timestamp. However, an audit conducted in June 2019 and highlighted the "need to improve "understanding" of the system among observers and general public" (Ehin et al., 2022, p.10, citing Rikk et al. ,2019).

Ehin et al. (2022) present that the share of the vote has risen with primarily every election, going from 1.9% of votes in 2005 to 46.7% in 2019. However, they also reported there was no boost in voter turnout. As of the 2019 national election, shown in Figure 1, the proportion of voters that trust the internet voting system is at 70%. When looking at other factors, they found that trust in the internet voting

system fundamentally drives online voting, regardless of other factors such as demographics or computer literacy.

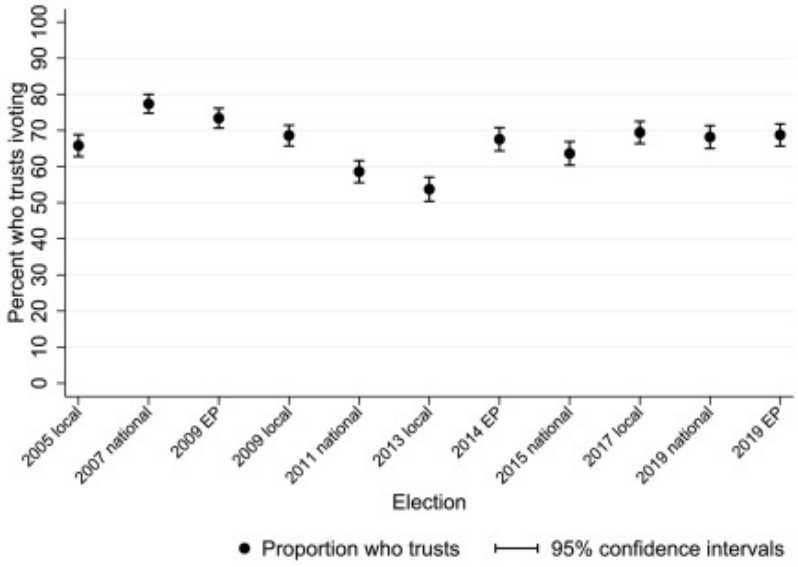

Figure 1 - Graph to show the percentage of the eligible voters from the Estonian population that trust their electronic voting system (Ehin et al. 2022)

The paper concludes that other countries have lost interest in internet voting due to fears of hacking and determined internet voting is incapable of being simultaneously transparent, verifiable, and private. In Estonia, internet voting is normalised, partly attributed to the acceleration of related technology within its nation before hacking and other attacks were more common. Additionally, they use many e-governance tools that have established trust, which helps build trust in related systems. The paper concludes that "strong digital identities" (Ehin et al., 2022, p.11) in their citizens are the key for governments to roll out their own successfully.

Overall, this paper shows how a nation can accept an internet voting system that runs alongside other voting options when digital tools are normalised and how this usage can grow over time. While mass acceptance like this is out of scope for this project, the paper successfully identifies the digital and socio-cultural landscapes required for governments to implement e-voting effectively. It demonstrated how homogeneity with neighbouring technologies must be considered when considering new voting systems.

Debate: safeguarding democracy during pandemics. Social distancing, postal, or internet voting—the good, the bad or the ugly?

Krimmer, R., Duenas-Cid, D. and Krivonosova, I. (2020). Debate: safeguarding democracy during pandemics. Social distancing, postal, or internet voting—the good, the bad or the ugly? *Public Money & Management*, pp.1–3. doi:https://doi.org/10.1080/09540962.2020.1766222.

This study was conducted in response to the COVID-19 pandemic and raised legitimate questions about how to maintain democracy when something external may confine people to their homes or cause them to be unable to be within a certain distance of other people because of their health.

It notes the choice between whether to hold an election or not and how the system needs to be adapted if held. The article examines each of these scenarios. They denote how adding health protection only, for example, guarantees a turnout decrease and potentially increases infection among the population from more potential exposures. Postal votes would eliminate the health risk for most of the population. However, they may put more health strain on postal workers during elections and would assume the postal system is unaffected by the conditions of the pandemic, which is unlikely. The final scenario is internet e-voting, which would not have delivery-related issues but has risks that require mitigation, making it not viable in the short term.

To conclude, this paper highlights the impact of elections when in-person paper voting may cause health risks to the population. It highlights the need to develop a long-term solution, such as internet voting, if an external event, like the Covid-19 pandemic, occurs again.

A Survey Based on Online Voting System Using Blockchain Technology

Shanthinii, S.P., Usha, M. and Prittopaul, P. (2023). A Survey Based on Online Voting System Using Blockchain Technology. pp.209–216. doi:https://doi.org/10.1007/978-981-19-7169-3_19.

Here, Shanthinii, Usha and Prittopaul (2023) state that “India is losing the genuine meaning of Democracy” (Shanthinii, Usha and Prittopaul, 2023, p209) because of the declining voter turnout. They argue that the only solution to combat this issue is to create a mobile or web application that citizens of India can use to vote in any location. Developing such an application, however, is not addressed in the paper.

The paper compares existing blockchain voting systems, focuses on Ethereum-based blockchain, and analyses its current potential and disadvantages. It concludes that Ethereum is an improvement on

other existing frameworks but requires more security, such as biometric ID checks using fingerprint scanners. The paper also discusses transparency as an ongoing issue but proposes no solution.

Overall, the paper establishes the potential of blockchain within e-voting systems using comparative study and makes clear it is not part of the problem, but further research is required to design a full end-to-end secure system. Despite referring to social issues in the abstract, the paper misses the opportunity to establish if this would indeed be a solution to India's voting participation problem and whether Indian citizens would be accepting of an e-voting system.

BieVote: A Biometric Identification Enabled Blockchain-Based Secure and Transparent Voting Framework

Faruk, J.H., Islam, M., Alam, F., Shahriar, H. and Rahman, A. (2022). BieVote: A Biometric Identification Enabled Blockchain-Based Secure and Transparent Voting Framework. *Fourth International Conference on Blockchain Computing and Applications (BCCA)*.

Identification is a theme mentioned in papers such as '*A Survey Based on Online Voting System Using Blockchain Technology*' (Shanthinii, Usha and Prittopaul, 2023) as a form of added security for an e-voting system. The BieVote shows how a blockchain-based e-voting system can be used with biometric identification technology (facial and fingerprint recognition) and asserts that the conceptual model presented will be further researched to create a "real-world application" (Faruk et al., 2022, p.7).

It conducted a literature review focused on Hyperledger Fabric-based blockchain systems with typical blockchain advantages, such as guaranteeing anonymity and decentralisation. The researchers use this form of blockchain to design the conceptual BieVote architecture that includes the biometric identification process to verify the voter's identity.

It examines how blockchain, a technology that prevents tampering with the information once stored, and biometric identification, a potential necessity to avoid voter fraud when voting from home, can create a stronger, more secure system. However, as it is only conceptual at this stage, verifying how much a system can satisfy all criteria, such as transparency, is difficult.

End-to-End Verifiable E-Voting Trial for Polling Station Voting

Hao, F., Wang, S., Bag, S., Procter, R., Shahandashti, S.F., Mehrnezhad, M., Toreini, E., Metere, R. and Liu, L. (2020). End-to-End Verifiable E-Voting Trial for Polling Station Voting. *IEEE Security & Privacy*. doi:https://doi.org/10.1109/msec.2020.3002728.

This study discusses a first-of-its-kind e-voting trial in the UK in 2019. It uses an example of an in-person e-voting system and receipt printing as part of the voting process. Testing an identification process was not a part of this trial, as researchers supplied participants with a random passcode to allow them to vote anonymously. Depending on how they tried to vote, they might walk out with up to one confirmed voting receipt and any number of cancelled voting receipts. It focuses on ensuring that voters feel confident that the correct vote they have selected is what they have cast and contains a system that confirms the cast votes and prevents mistakes in casting. The usability of the system had an excellent score.

A survey was held for each voter after using the machines, with 93 returned surveys. More than half the participants stated they preferred the e-voting system as the method felt “easy” and “safe” (Hao et al., 2020, p8). However, some participants still felt the security of e-voting was an issue and maintained their preference for paper ballots. Many who felt neutral also stated that e-voting in person felt no different to voting by paper and would prefer to vote remotely (Hao et al., 2020). These results have limitations, such as the survey size and were limited to those local to the study location.

What is missing from this paper is whether it was easy and safe for voters to verify their vote and understand how it works. Their configuration for receipts uses a long string of letters and numbers for confirmation, which would be meaningless to the voter and may not be trustworthy to them. Additionally, the cancelled ballot clearly shows the candidate's name on a cancelled vote, which could violate our established receipt-free criteria.

Figure 2 - Image showing the difference between a cancelled and confirmed ballot in the e-voting trial (Hao et al. 2020)

Electronic Voting System Using an Enterprise Blockchain

Denis González, C., Frias Mena, D., Massó Muñoz, A., Rojas, O. and Sosa-Gómez, G. (2022). Electronic Voting System Using an Enterprise Blockchain. *Applied Sciences*, 12(2), p.531. doi:https://doi.org/10.3390/app12020531.

This paper outlines potential flaws of existing electronic solutions that use a centralised approach instead of blockchain, including how data can be manipulated intentionally or by accident. It notes existing problems with permissionless blockchain as a solution, such as high-power consumption and how the model presented in the article can tackle all these issues. It discusses using Enterprise blockchain to create a secure system that preserves voters' privacy, is more efficient, and can decrease vote counting time.

The paper presents several criteria in the introduction to what those who run as candidates or vote might require of an e-voting system. These themes arise in many e-voting papers, but what is notable is the receipt-free criteria - that a vote should not create a receipt as it may be problematic to produce something that could show how a voter voted. The research by Hao et al. (2020) demonstrates that this does not necessarily mean physical receipts are not a possibility in a voting system, but only that any

party can use the receipt to prove how they voted. The paper does not explore the issue of transparency and how easily a voter could understand the system presented in the paper.

A Self-Tallying Electronic Voting Based on Blockchain

Zeng, G., He, M., Yiu, S.M. and Huang, Z. (2021). A Self-Tallying Electronic Voting Based on Blockchain. *The Computer Journal*. doi:https://doi.org/10.1093/comjnl/bxab123.

Zeng et al. (2021) present the problem of blockchain-based systems requiring a central representative to count votes or limit the number of countable votes. However, blockchain has advantages, costing $0.70 per voter when using an Ethereum blockchain system, compared to $2.77 using paper. In response, the paper presents a solution to this problem by creating a self-tallying system.

Compared to other schemes, the proposed system is more secure and does not need to trust an independent third party to complete the tallying. However, a new problem arises: whoever the last person to vote is will know the total number of votes ahead of time and may amend their vote based on this information, denoted as “last voter privilege” (Zeng et al., 2021, p3030). The paper discusses potential workarounds but concludes that this is an unresolved issue.

Overall, the system has clear merit based on its advantage compared to others within the paper. It also explored the cost differences in blockchain technology. However, it is still not a perfect solution – requiring further research and development to find a full resolution.

E-voting in Nigeria: A survey of voters’ perception of security and other trust factors

Osho, O., Yisa, V.L. and Jebutu, O.J. (2015*). E-voting in Nigeria: A survey of voters’ perception of security and other trust factors*. IEEE Xplore. doi:https://doi.org/10.1109/CYBER-Abuja.2015.7360511.

Osho, Yisa, and Jebutu (2015) performed this survey in 2015 after Nigeria implemented partial e-voting for the first time. The paper details how the existing method of conducting elections was losing trust and, therefore, required new ideas and approaches to regain vote integrity.

The survey found that many participants would prefer to vote electronically, except those who reported low IT proficiency. It claims that significant effort would be required to increase trust among this demographic of voters, and any e-voting system must maximise its ease of use. To enhance this trust, they

describe how e-voting systems must have five factors: “privacy, reliability, ease of use, security, and availability” (Osho, Yisa and Jebutu, 2015, p.207). There is also the need to increase the proportion of Nigerians who have access to the Internet for e-voting to be successful (Chikioke-Keme, 2019).

One drawback to the survey is the minimal diversity in the participants, as most were young males, with just over half describing themselves as IT proficient. This survey is also nearly ten years old, and technological advancements may impact how participants view security and trust.

Formalization of Receipt-Freeness in the Context of Electronic Voting

Bräunlich, K. and Grimm, R. (2011). Formalization of Receipt-Freeness in the Context of Electronic Voting. 2011 *Sixth International Conference on Availability, Reliability and Security*. doi:https://doi.org/10.1109/ares.2011.25.

Receipt-freeness is the idea that after voting, a voter cannot possess any form of receipt that can reveal how a ballot was cast, which is vital in maintaining secrecy and protecting voters. This paper focuses on presenting a security model that explicitly targets receipt-freeness. It also refers to the “Common Criteria for Information Technology Security Evaluation (CC)” (Bräunlich and Grimm, 2011, p.119) that uses a scale to evaluate the level of assurance of security for a system. It notes that the score must reach a higher threshold for elections than for non-election e-voting systems.

The security theorem in the paper states that if a voting system is secure in terms of receipt-freeness and a set of four rules are satisfied for the data in transmission, then the voting system is secure. The researchers draw the rules, constraints, and definitions from various academic sources. The model presented could satisfy a high CC evaluation.

Finally, the paper recommends that the next step in the research is to formalise verifiability for both the individual voter and the general population to highlight any conflict between this voting requirement and receipt-freeness.

Coercion-Resistant E-Voting Scheme with Blind Signatures

Ahsan, A. (2019). Coercion-Resistant E-Voting Scheme with Blind Signatures. *2019 Cybersecurity and Cyberforensics Conference (CCC)*. doi:https://doi.org/10.1109/ccc.2019.00009.

Ahsan (2019) proposes a different e-voting scheme, utilising blind signatures - a possible solution to some of the security requirements for e-voting. The paper defines coercion-resistance as having receipt-freeness and that any potential individuals that would coerce other voters are not given the opportunity, via voting preference or voting omission.

The system allows a voter to create a genuine login and many fake logins with various passwords. The system ignores any votes committed with fake logins; only those cast with a genuine login will succeed. Steps are taken within the design to ensure this cannot be detectable in all realms, and bad actors cannot request fake passwords in excessive bulk.

The paper proposes a system that would avoid coercion; however, vote verifiability still exists at an individual level, which this model does not cover. It states that coercion-resistance conflicts directly with the verifiability property “tallied-as-recorded” (Ahsan, 2019, p149), where voters would require the ability to check if the tally includes their cast vote. The paper concludes that this model could not work as-is for an end-to-end verifiable system (Ahsan, 2019, p149).

2.4 Theory

Multiple papers have explored designing systems that include blockchain, which solves criteria such as ensuring votes can remain unchanged and be counted accurately. However, a prominent theme in prior literature is to find a solution to voter verification so that voters can be confident they have voted as intended and trust their vote is counted - without risking their anonymity or privacy.

Faruk et al. (2022) has demonstrated how blockchain and an identification system can be part of the same framework of an e-voting model. Since UK elections now require that photo ID be provided to vote, we and must build this into the working prototype to be compatible with the UK process. Although required regardless, using an online identification system with biometric technology would also enhance both security and privacy for the identification process (Faruk et al., 2022).

Ensuring a solid understanding of how an e-voting system operates, as well as keeping receipts easy to understand and confidential (Abuidris et al., 2019), can be a barrier to ensuring their anonymity and

privacy are safe. Survey participant feedback refers to security and the need for assurance that their vote is safe (Hao et al., 2020). A theory on how this problem could be solved is presented in two parts:

- If a voter can use a secret word chosen by them to "see that is their vote" (Abuidris et al., 2019, p.367) online this would allow the voter to be reassured their vote is correct while keeping receipts easy to understand and confidential.

- If a timeout feature is added to the verification function so that it can only be done moments after voting, this would avoid coercion and receipt abuse.

Our literature base shows how the level of e-voting usage is driven by trust of the e-voting system (Ehin et al., 2022). The verification method is vital to establishing trust (Abuidris et al., 2019), and it should be easy to use (Osho, Yisa and Jebutu, 2015). There is also, however, a need to understand how the e-voting system works (Ehin et al., 2022), particularly so that users can assess the tool's effectiveness themselves (Jafar, Aziz and Shukur, 2021). Therefore, it is theorised that including information about the functionality of blockchain will help improve this understanding and, combined with the secret word style verification system, is expected to improve trust in the e-voting system. Analysing participants' engagement with the prototype via a thorough evaluative section on these concepts will demonstrate if this is the case.

2.5 Terminology

E-Voting: In the context of this paper, this refers to internet electronic voting, or rather voting online via the assistance of the internet, unless otherwise specified.

Hash: Refers to the definition in the subject area of blockchain. They are fixed length strings created through designated encryption that are impossible to guess (Frankenfield, 2019).

NGO: Non-Governmental Organisation

URL: Uniform Resource Locator

2.6 Chapter Summary

This chapter establishes that no complete system yet fully satisfies the agreed criteria for an e-voting system in the UK, and the contradictive nature (Ahsan, 2019) of some of the requirements.

To summarise, the criteria required for an internet e-voting tool is as follows:

- Verifiable votes that do not jeopardise privacy or risk coercion
- An ID system that prevents voter fraud but keeps anonymity safe
- Votes are secure, accurately recorded and the count of votes can be proven
- The tool is accessible to potential voters

These ultimately are expected to lead to trust in the tool, which in turn, leads to its usage (Ehin et al., 2022). As a result, an area of focus will be verifiability, and the benefits that come from users being able to view their successful vote, as well as how this could be achieved whilst preserving privacy and the benefits of receipt-freeness. The next chapter will begin to convert the criteria and proposed theories into a complete design for the IT artefact.

Chapter 3. ANALYSIS AND DESIGN

3.1 Chapter Introduction

Through the literature survey and research, blockchain has shown considerable potential within e-voting systems in practice and theory. While issues remain around user understanding and overall public trust in a complex technological system, combined with other methods, it could become more than the sum of its parts.

This chapter will now take the theory established in Chapter 2. and translate this into a technical specification for a new e-voting prototype. It will go into detail of the design and describe how data will be gathered for evaluation. The design will uphold the features and attempt to satisfy the identified criteria to achieve this project's aims. What is clear is that quantitative simulations alone are insufficient to evaluate this tool. Many of the issues raised around trust and transparency are social issues, and henceforth, a survey will also be designed in this chapter to lead to a comprehensive evaluation of the prototype.

3.2 Project Specification

Our concept of an e-voting prototype that enshrines core democratic principles must heavily rely on our previously stated aims and what was learned from prior literature. In addition, using UK election statutes determines part of how an e-voting prototype must behave, in the form of:

- a mandatory identification check for voters
- secure infrastructure
- upholds the privacy and anonymity of the voter, maintaining secrecy and avoiding coercion where possible

Using these and those demonstrated possible in prior research, this project will include creation of an IT artefact to act as an internet e-voting tool prototype. To achieve our stated aims, the following features will be included:

- Remote access through the internet

- Instructions on how to vote and information about the candidates
- A remote solution to identification to determine eligibility
- Immutable vote casting
- Information on how the technology of the artefact works
- Allows only those eligible to vote, including preventing those who have already voted from voting more than once. These features minimise system abuse whilst maintaining anonymity.
- A self-verification system for votes cast using a secret word and timeout system such that a third party cannot later use to identify how someone voted.

Alongside the design and creation of the artefact, we will design a survey to test the tool, simulate a vote, and test if the verification process works from a technical standpoint. All of this will work towards answering the problem statement questions.

3.3 Research Methods

The first research step will be to identify the resources for development that can successfully satisfy all required functions for the artefact, which will be detailed in this chapter. Once the IT artefact has been designed and created, two main data-gathering methods will be used to conduct the research for the IT artefact evaluation.

- **Survey:** A vital feature of this project is to find if users could trust an e-voting model, and the best way to achieve this is by asking them. The survey will be conducted remotely and advertised online.
    - For the survey questions, this data will be analysed quantitively, with some qualitative analysis of open survey questions. This mixed-method approach will give a better understanding of people's concerns with the prototype and whether they find it trustworthy.

- The tool will be hosted and accessed online during the survey questioning for additional testing. Participants of the survey will, therefore, be able to use the tool as it would likely be deployed in a real-world implementation and complete a vote simulation simultaneously during their survey participation.

- **Security Tests:** In addition to the simulations through the survey testing, the blockchain and biometric identity functions that comprise the back-end functionality will be extensively tested to gather results around their accuracy and consistency. This is to establish if the IT artefact is functional and achieves the aims it has set out for it.

3.4 Design Considerations

3.4.1 Overview of IT Artefact Design

The tool will be an online web application that can be accessed remotely, and the informational requirements will be easily incorporated using text on the screen for the user to read. To protect the survey participants' data, answers should be anonymous and not require the storage of any personal data. Therefore, a full version of the prototype that includes the photography of their identification and collection of their name and address to compare would not be appropriate for this research. Consequently, this design will have two versions of the IT artefact: a complete version with all working features and one that omits the identification steps for testing. Both will still incorporate blockchain and have identical workflow structures. For the test version, a screen describing how an ID check will occur at that time will be used instead of an actual check.

This project will incorporate blockchain technology at the centre of the design and will include the proposed self-verification element to help foster trust within the potential voter. The specific design for the features is as follows:

- **Anonymous eligibility checking:** Two separate databases for voters and votes so no party in the system can link the votes to the original voter. The identification process is entirely separate from the voting process.

- **Remote identification:** Biometric identification technology will identify the voter within the e-voting tool. This will include facial recognition and text recognition technology to compare a user's face and electoral registration information to their photo ID.

- **Immutable vote casting:** As previously established, blockchain is used in many e-voting models and is a way in which votes, once stored, cannot be changed.

- **Description of how the tool works:** For this project, blockchain is part of the back-end design and so an explanation of how it works will be incorporated into the tool in the front-end.

- **Self-verification:** The self-verification system works by asking the voter for a secret word, whereby there is a short amount of time when the voter can check that the vote they cast is the same as they intended. Once this period has passed, the individual voter can no longer view how they voted directly.

The tool is designed in the following structure, as seen in Figure 3 - Flow chart demonstrating the back-end structure of the IT artefact.

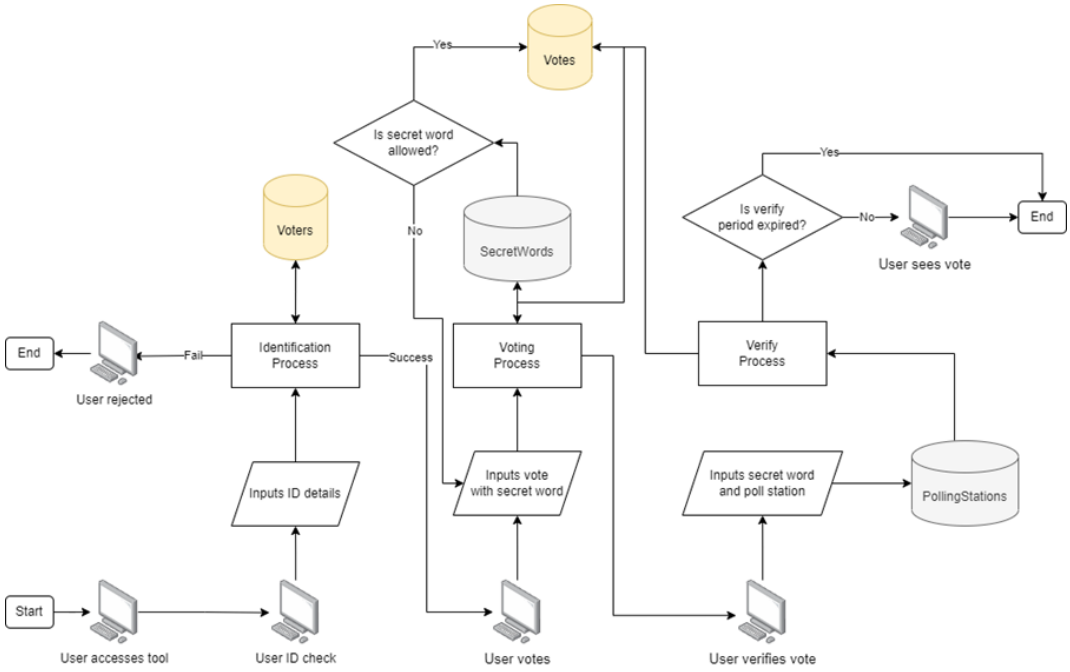

Figure 3 - Flow chart demonstrating the back-end structure of the IT artefact

3.4.2 Pseudocode

The pseudocode below describes the design of the IT artefact:

```
Check voter eligibility:
Receive input:
   [voter poll number or full name and address]
          Call database ‘voters’ - GET and store as variables (pollnumber,
          pollingstationprefix, fullname, address, votingeligibility,
          hasvoted)
          If voter not in database:
                Voter eligible fail - User not found
                End
          If votingeligibility is not eligible:
                Voter eligible fail - User not eligible
                End
          If voter hasvoted is yes:
                Voter eligible fail - User already voted
                End
          Else:
                Voter eligible success
   Check voter identification:
   Receive input:
          If id information matches user:
                Voter identified success
          Else:
                Voter identified fail
                End
   Check secret word:
   Receive input:
          [secret word]
          Call database ‘secretwords’ - GET (secretwords)
          If secret word in database:
                Reject word and show error message on screen
          Else:
                Continue
   Voter votes:
   Receive input:
          [details of vote and secret word]
          Concatenate pollingstationprefix and secret word (votingreference)
          Encrypt details of vote and votingreference
          Call database ‘votes’ - POST (votingreference, details of vote,
          timestamp)
          If POST successful:
                Update hasvoted to yes
                Call database ‘voters’ - PUT (pollnumber, hasvoted)
                If PUT Successful:
                Else:
                      Retry
          Else:
                Retry
   Voter verifies vote:
   Receive input:
          [secret word and (polling station or address)]
          If received address:
                Call database ‘pollingstations’ - GET pollingstationprefix
          Concatenate pollingstationprefix and secretword (votingreference)
          Encrypt votingreference
```

```
Call database ‘votes’ - GET votingreference, timestamp, votedetails
If timestamp + allowed_time > Now:
       Verification fail - outside of time window
Else:
       Decrypt vote details and display on screen
       Expire window after 30 seconds
```

3.4.3 User interface and Technologies Used

The artefact will be produced using Python, HTML and CSS to create an online web application that survey participants can access. The researcher has extensively used all three languages, so has the existing skillset to create a web-based application to house and run the IT artefact. Whereas building blockchain databases and identification checking will require some further skill development, as much of the complexities with integrating into a prototype have not been explored.

Python has been chosen as the language, as it can easily develop blockchain databases and has available open-source technology for identification checking. It will form the back-end functionality using the open-source package Flask. Flask was chosen due to the simplicity and enables developers to rapidly create web applications to test out ideas, and flexible works with other libraries (Ranjan, 2023). PythonAnywhere will host the application for remote access as it is gives the ability to host Python projects remotely via a browser (PythonAnywhere, 2022). For the database component, the open-source package sqlite3 will be used for storing data within the application, as it can create lightweight self-contained databases (Summit, 2023) which suits the requirements for this application.

Although the back-end incorporates some complex components, the design for the user interface will be simple and accessible, guiding the user on how to use the tool. This is because of established concerns around easy of use being a requirement to trust the tool (Osho, Yisa and Jebutu, 2015). As a result, the front-end requirements will be simple to keep the tool easy to understand and use. Figure 4 - Example wireframe of the user interface for the IT artefact voting pageshows an example wireframe of how the voting screen may look. HTML and CSS will be used to render the application's front-end as they are the most common language for webpages and most browsers support HTML (BIJU's Future School, 2021).

Figure 4 - Example wireframe of the user interface for the IT artefact voting page

Other areas of technology used include the survey using Microsoft Forms as the data is encrypted at rest and in transit (Microsoft, 2023). The survey results will be analysed using Power BI to visualise the data in a digestible format. Finally, the code repository will be hosted on GitHub for change control.

3.4.4 Evaluation

The evaluation will test three main hypotheses based on the problem statement questions.

$H_{0\text{-}1}$ The e-voting tool can identify a user is who they claim to be.

$H_{0\text{-}2}$ The e-voting tool is entirely secure and cannot be tampered with undetected by the public or the government.

$H_{0\text{-}3}$ Voters trust the e-voting tool.

The first two hypotheses will be tested statistically by running the following simulations:

- A simulated election using test identifications will determine if remote identification has merit in this context. A threshold for accuracy will be established to pass.

- A simulated ‘hack’ or attempt to alter the data will test if tampering is possible and, if so, if it is easy to identify. The test will involve attempting to change data when committing to the block-chain.

For the third hypothesis, survey answers by test participants who have reviewed the IT artefact will be used. The complete design of the survey is detailed in the next section.

3.4.5 Survey Design

The survey questions aim to test if identification can be effective, security can remain uncompromised, and both sides can uphold two-way transparency. Developing and evaluating an e-voting tool with this design will answer these questions.

The survey will consist of anonymous responses, where information is collected before and after a test of the IT artefact. To ensure everything is anonymous, the artefact used in the survey will be a test version that does not require the collection of identification. There will be questions around identification when voting in general and an obvious explanation within the artefact to demonstrate how a completed version would act in a finalized version instead. The majority of questions will have only a closed set of answers, such as “Yes/No” to allow for quantitative analysis. Some of these closed questions will use Likert scales to capture and measure the opinions of participants, from “Strongly Agree” to “Strongly Disagree” (Bhandari and Nikolopoulou, 2022). However, there will also be an opportunity for participants to provide feedback through open questions with free text to supplement. The survey is split into sec-tions, with some gated responses for those already familiar with blockchain and e-voting.

- **Screening:** This section removes anyone under eighteen or who has never voted. By restrict-ing later question to only those who had voted in the UK before, all participants could make a fair comparison between the existing voting system and the potential one within the artefact.

- **Background:** Basic questions such as age and experience in voting to test if changes exist in those within different groups.

- **Electronic Voting (before):** Gated questions only for those who have heard of electronic voting to capture their thoughts and understanding of the subject before testing. These function as a control to establish if the tool impacts these opinions.

- **Blockchain:** Gated questions for only those who have heard of blockchain to determine if the survey participant could explain it. Again, this type of question acts as a control for when the participant then goes on to assess the tool and read about blockchain.

- **ID:** A question on the new identification measures in the UK to determine how participants feel about the recent change and if this relates to how they would feel about implementing e-voting.

- **Artefact test:** The survey participant will also test the software at this stage. When the participant completes the test, the word 'CANDIDATE' will be shown on the screen, which the participant must provide in the screening question within the survey. This word was chosen due to it being easy to remember but not easily guessed unlike something like 'complete' or 'thank you.' Adding this ensures that those who completed the survey are all participants who finished the test. Results will exclude anyone who does not provide this word.

- **Artefact review:** The review will include questions about the ease of use and understanding of the artefact, as well as if their understanding of blockchain has improved. These questions are imperative to determine if the artefact could be trusted.

- **Electronic Voting (after):** These allow the results to compare the participant's answers before and after the tool's test. This comparison is to determine if there has been an impact on their initial thoughts and knowledge.

- **Concluding:** This section is for a qualitative analysis of the opinions of electronic voting and how it may be beneficial or concerning. This is an opportunity for users to wrap up their thoughts and provide any further feedback not already been asked of them.

The survey is estimated to take 10-15 minutes to complete and will provide results on whether a participant could trust the artefact enough for the concept to be considered in future solutions. Once

completed, the survey results will be imported into Microsoft Power BI and transformed to produce meaningful analysis and compare changes to participant viewpoints of both electronic voting and block-chain.

The researcher will source participants using promotion to online networks with no provided incentive. All responses will be anonymous, and all data will be transferred from Microsoft Forms and kept on the University network drive. Once the project is completed, the data will be destroyed.

3.5 Chapter Summary

At this stage, the design for the IT artefact has been established, considering the requirements detailed in Chapter 2. It has identified the technical aspects of the design and how these will be executed to create a piece of prototype software. With the design in place, the project is poised to explore a new model for internet e-voting that can attempt to solve previously unsolved criteria.

For evaluation, a mixed-method approach using a combination of data-gathering methods is appropriate for establishing if the project will meet its aims. The tool will undergo back-end tests and checks to meet security and accuracy requirements. The survey section will tackle several areas, including established views on e-voting and blockchain, a live prototype test, questions around concerns to measure opinion, and the opportunity to write feedback in their own words. The next chapter will begin to bring this design to life.

Chapter 4. IMPLEMENTATION (REALISATION)

4.1 Chapter Introduction

Development of the internet e-voting tool was created in two phases: a preliminary phase to implement a test version of the tool for the survey, and a secondary phase to fully develop the tool to have all features given in the design. The previously stated design was used as the template to begin the IT artefact, which subsequently involved some minor changes and additions, detailed throughout this chapter to execute a fully successful prototype. Fundamental ideas, however, remained unchanged throughout and the e-voting tool was completed with all designed functionalities. In this chapter, final implementation of the artefact will be detailed, along with the steps taken to reach a fully executed application.

4.2 Details of the Implementation

Since two versions of the application were required for development, there are two scripts in the directory, app.py and app_test.py The full code for these can be found in Appendix 6.7D.1.1 and 6.7D.1.2 Throughout this chapter, all features can be assumed to apply to both versions, except for where indicated.

Repository directory structure:

```
C:.
├───__init__.py
├───app_test.py
├───app.py
├───blockchain.py
├───identification.py
├───LICENSE
├───README.md
├───requirements.txt
├───databases_test
│   ├───voters.db
│   └───votes.db
├───idphoto
├───instance
├───static
├───templates
└───test
    ├───results
    ├───test_images
```

```
├──blockchain_test.py
└──identification_test.py
```

4.2.1 Flask and User Interface

A completed web application was successfully built using the *Flask* package in Python and works by creating an application script containing routes that can be called from within the browser. For this project, there are two application files, *app_test.py* and *app.py* relating to the two respective versions of the tool. These scripts form the website's back-end and define actions when different pages are routed to the website. A *'templates*' folder contains the HTML code for rendering the front-end, with a stylesheet stored within.

The code extract below shows how a route is created, using the check eligibility route as an example. A function is created under the route to instruct the application on what to do when the route is called. In this example, when the application routes to */checkeligibility*, the *'voters'* database is called to then feed respective test credentials for selection; it feeds this into the 3_checkeligibility.html template from the *'templates'* folder. All functions pulled from route functions are defined earlier in the application script or imported from other Python files, such as the blockchain.py file.

```
# Placeholder for providing your poll number or name and address to check eligi-
bility (must come before ID check)
@app.route("/checkeligibility")
def checkeligibility():
    # Connect to voters and get full list
    voters = r"databases_test\voters.db"
    select_all_voters = "SELECT * FROM voters;"
    conn = connect_to_database(voters)
    result = execute_sql_fetch_all(conn, select_all_voters)
    conn.close
    return render_template("3_checkeligibility.html", test_voters = result)
```

User interfaces used only HTML and CSS languages, as designed, with only one small exception. A small amount of Javascript became necessary for the *5a_idphoto.html* file to use and render a connected webcam, enabling the application to store and use photos for the identification process. UI design is mainly defined in the *0_index.html file*., which is extended in other templates using the block content feature. Using the block extension method, allows the header and footer to remain consistent across the site, keeping a consistent feel through.

```
{% extends '0_index.html' %}

{% block content %}

… content goes here

{% endblock %}
```

Figure 5 - Homepage of the implemented artefactshows the full version homepage of the IT artefact. The test version has slightly different templates for some pages, with changes to the wording for the survey; but functionality remains identical. In Appendix 6.7D.4, test versions of templates files are all suffixed with *'…test'*.

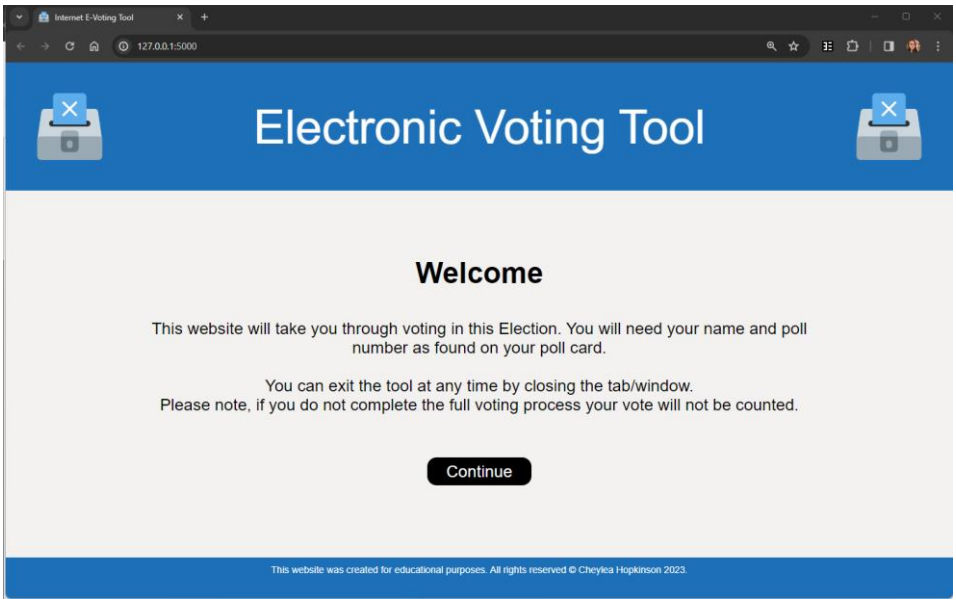

Figure 5 - Homepage of the implemented artefact

For some routes, information is required to be passed into the URL (such as the poll number and secret word). These are indicated in the route string, as seen in the example below for */verifyid.*

```
# Placeholder for identification process in full version of the artefact
@app.route("/verifyid/<pollnumber>")
def verifyid(pollnumber):
    # Connect to voters and their details for screen display
    voters = r"databases_test\voters.db"
    pollnumber = decrypt(key, pollnumber) # decrypt for database
    select_voter_details = "SELECT name FROM voters WHERE pollstation ||
CAST(pollnumber as text) = '" + pollnumber + "';"
    conn = connect_to_database(voters)
    result = execute_sql_fetch_one(conn, select_voter_details)
    conn.close

    pollnumber = encrypt(key, pollnumber) # encrypt for url
    return render_template("5_verifyid.html", name = result[0], pollnumber = poll-
number.decode('utf-8'))
```

When this occurs, it is encrypted, before passing the information into the URL to avoid information being directly read from it. This is achieved using the encrypt and decrypt functions found in both app files (see 6.7Appendix D.) using Fernet from the *cryptography.fernet* package. The key for this encryption isn't stored directly in the code but outside it in a *config.py* file, for added security. This package was specifically chosen for its simplicity and effectiveness for keeping data secure (Lake, 2023).

```
### Encryption Functions ###
def encrypt(key, message: bytes):
    """Encrypt the provided variable

    Key arguments
    key -- key to encrypt with
    message -- the value to be encrypted
    """
    message = message.encode()
    return Fernet(key).encrypt(message)
```

4.2.2 Database Design

An original design depicted four databases to hold all the necessary data for implementation. When developing the project, it became clear that it was only necessary to have two databases to house *'votes'* and *'voters'* data separately, making data easier to work with. The final table diagram detailing entity relationships can be found in Figure 6. In this case, no table has a direct relationship with any other table, so there are no foreign keys on the tables.

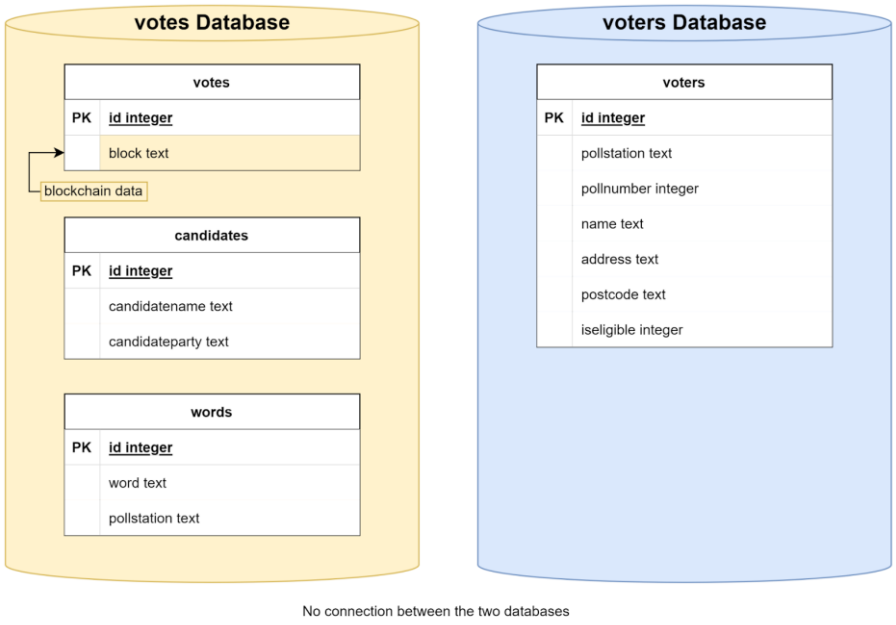

Figure 6 - Entity relationship diagram showing the final database structure for the implemented artefact

Each table in the two databases is related to the original design, where these were originally planned to be their own individual databases. As in the design, these are created using the Python *sqlite3* package and are contained within the application. Upon initialisation, the databases are built inside the tool using test data only. For the application to connect to the databases during its use, some functions are defined at the top of both app files for connecting and querying the database:

- *connect_to_database*: Takes the location of the database as a parameter and opens a connection to the database.
- *execute_sql*: Executes SQLite script on the open connection, taking the connections and SQL string as parameters. Used to set up all the tables at initialisation.
- *execute_sql_fetch_one*: Used to select one answer from a database
- *execute_sql_fetch_all*: Used to select multiple answers from a database

The code extract below shows how this is executed for the table *'words'*.

```
# Create tables for the votes database
votes = r"databases_test\votes.db"

...
```

```
# Table that stores words that cannot be used as secret words
drop_table_words = """DROP TABLE IF EXISTS words; """
create_table_words = """ CREATE TABLE IF NOT EXISTS words (
                                id integer PRIMARY KEY,
                                word text,
                                pollstation text
                            ); """
# Insert banned words
insert_table_words = """ INSERT INTO words (id, word, pollstation)
                              VALUES
                                (1, 'TEST', 'all'),
                                (2, 'CHARLIE', 'all'),
                                (3, 'VOTER', 'all'),
                                (4, 'SAM', 'all'),
                                (5, 'BAILEY', 'all'),
                                (6, 'EXAMPLE', 'all');
                            """

# Make connection to voters database file
    conn = connect_to_database(votes)
    if conn is not None:
        # Execute required sql
        ...
        execute_sql(conn, drop_table_words)
        execute_sql(conn, create_table_words)
        execute_sql(conn, insert_table_words)
        ...
        print("Votes database complete.")
    else:
        print("Error, no connection.")
```

- **‘votes’ Table:** The votes table consists of an id index and a column to store the blockchain block in the JSON format. The details for the information in the block are in section 4.2.4.

- **‘candidates’ Table:** This table contains the candidate names and party to be rendered in the front-end and stored within the vote.

- **‘words’ Table:** This table contains *id, word* and *pollstation* columns. The words included at the beginning are all identifiable names and street names found in the electoral roll information, so these cannot be used as secret words. This could also be extended to offensive terms. When a person casts a vote, their secret word alongside their poll station is recorded to prevent people from using the same secret word within a given poll station. This was restricted to poll stations to avoid user friction as an election progresses, as an increasing number of wards become unavailable. Any words prevented in all poll stations are marked as “all” in the poll station column.

- **‘voters’ Table:** This contains all the personal information required for a voter to cast their ballot, including their poll station, poll number, name, address, postcode and whether or not they are eligible to vote. This is a true/false column, and once a vote is completed, this is updated to false. It is possible for this to begin as false if the voter is not eligible for other reasons, as is the standard in current elections.

When using the databases in the application, the defined functions are run when called by the route functions. An example could be displaying all party candidates on one screen, as seen in the code extract below.

```
 Screen to vote
@app.route("/vote/<pollnumber>/<secretword>")
def vote(pollnumber, secretword):
    # Connect to voters database to get list of candidates to vote for
    voters = r"databases_test\votes.db"
    select_all_candidates = "SELECT * FROM candidates;"
    conn = connect_to_database(voters)
    result = execute_sql_fetch_all(conn, select_all_candidates)
    conn.close
    return render_template("7_vote.html", candidates = result, pollnumber = poll-
number, secretword = secretword)
```

In a fully finalised implementation of this artefact, the ‘*votes*’ blockchain table would need to broadcast to other databases on a peer-to-peer network, but this is outside this project’s conceptual scope.

4.2.3 Identification (app.py only)

Contained in the application is a Python file called *identification.py*, which holds the Identification class information and used within the full version of the application *app.py* only. It includes the following functions:

- *check_identification_text*: accepts an image path and comparison name and address, then scans a provisional or full UK Driving licence and will return two similarity percentages for the name and address.

- *check_identification_face*: accepts an image path only and opens the webcam to check the face in real-time and compares it to the provided image. If there is a match, this is returned as a pass, or it will expire with no matches after two minutes and will return a failure.

A full code extract for these functions can be found in 6.7D.1.4 , with both inspired by articles by Stratis (2023) and Yadav (2023).

The text comparison function uses *Image* from the Python Imaging Library (PIL) package (Lundh and Clark, 2011) to open the image, the *pytesseract* package (Lee, 2023) to convert the image to a string of text and *SequenceMatcher* from the *difflib* package (Drake, 2024) to check the similarity between two text strings. For face comparisons, the *face_recognition* package (Geitgey, 2020) is used to identify a face in the provided image and return an error if it is not found. These packages were chosen based on their open-source nature and the established use case in their respective articles.

4.2.4 Blockchain

The application contains a Python file called *blockchain.py*, which creates the Blockchain class, used in the main application files. The class consists of the following:

- *__init__:* to create the first block in the chain and set it to zero.
- *create_block*: to create subsequent blocks
- *proof_of_work*: get proof of work to mine a new block
- *hash*: get the hash calculation for the block

These functions are called from the app files to create vote blocks, then stored in the vote database. The class also contains a function for checking the chain validity which is used later for testing. All functions were inspired by the article by Geeks for Geeks (2023), '*Create simple blockchain using Python*'.

The first block will have a previous hash value of 0 and no data, while any subsequent block in the chain will contain details on the vote and the hash.

id	block
1	{"index": 2, "timestamp": "2024-01-05 23:28:16.581903", "proof": 1, "voter": "nonenone", "candidate": "none", "previous_hash": "0"}

2	{"index": 3, "timestamp": "2024-01-05 23:28:17.804141", "proof": 632238, "voter": "ABCHELLO", "candidate": "Emma Candidate", "previous_hash": "329f76c40f1fea236533a2c89ca1d4c279fff5e387dd118c3323bfb276e0f7e3"}

Table 1 - Table showing the first and second block in a blockchain produced by the IT artefact

The information stored in the blockchain is used for the artefact's functionality.

- *timestamp*: to capture when the vote was cast so that self-verification can be prevented when a certain period has passed
- *proof*: for proof of work validity
- *voter*: the secret word with the poll station so this can be used to verify the vote after casting. This is not identifiable to any third party.
- *candidate*: to record who the vote is for
- *previous_hash*: the hash value for the previous block

The packages used to create the functions include *datatime* to account for the timestamp, *hashlib* for hash calculations and *json* to store data. As with identification functions, these were chosen due to the established use case in the Geeks for Geeks (2023) article.

4.3 The IT Artefact

The IT artefact is a web application that executes an e-voting process from webpage to webpage. This section will break down different elements of the application and how each part works and is interlinked.

4.3.1 Home and Frequently Asked Questions

User journeys begin at the Home page of the website, which welcomes the user to the voting process, as seen in Figure 5 - Homepage of the implemented artefact. While the flowchart in Figure 7 - Diagram to show the workflow for Home and FAQsshows how users navigate from the Home screen to the Frequently Asked Questions (FAQs) page, and the routes called in the application.

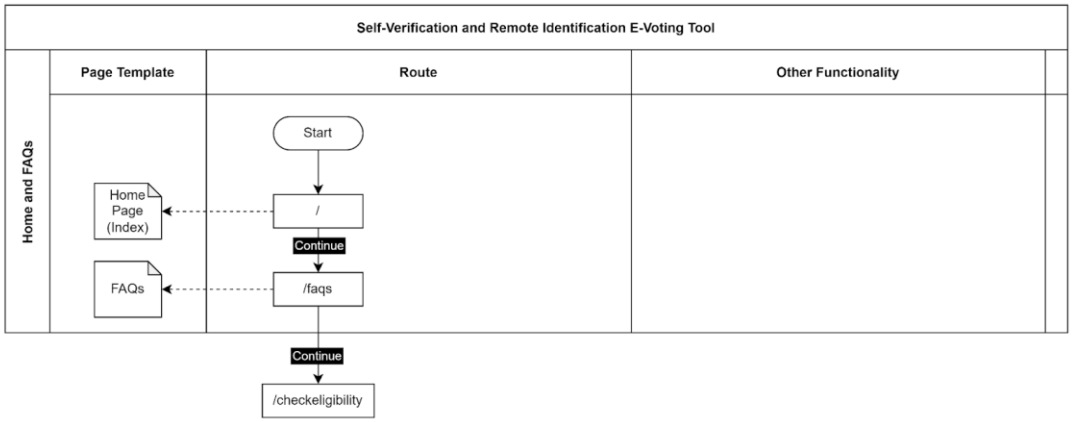

Figure 7 - Diagram to show the workflow for Home and FAQs

The FAQs page conveys to the user how the tool works. This was an essential addition to the artefact to check the users understanding. FAQs and answers are provided as follows:

- **How does the voting work?:** The voting tool will first check if you are able to vote and perform an identity check. You can then select a candidate to vote for. When voting, you will be asked to provide a secret word. Once you cast your vote, a technology called 'blockchain' is used to record your vote such that it can't be changed. For five minutes after voting, you will be able to view the candidate you voted for. This is a way of verifying the correct vote has been cast by using your secret word.

- **What is blockchain?:** Blockchain is a way of storing data. Pieces of data are stored in 'blocks'. Once stored, they cannot be changed. Each block contains data that can connect it to the previous block. This means data is stored as a chain of block data that only has one order. Votes are collected without your personal data. Instead, a secret word of your choosing is used to maintain the anonymity of your vote. When storing the blocks, these are published in multiple places. This means people will be able to see and view the data stored when your vote is collected.

- **How can I know my vote will be counted correctly?:** Blockchain data cannot be changed. Once your vote is stored, that is the vote that will be counted. This tool allows you to view your unchangeable vote after it is stored. This is so you can verify the vote is the candidate you selected. This is only available up to five minutes after you cast your vote and will require you to remember your secret word.

- **What can I use for my secret word?:** You can use a word or phrase up to 15 letters. However, you can't use any names of other voters or addresses. You also can't use a word that has already been used by another voter at your polling station. Try to choose something easy to remember. Please be aware, if you forget your secret word you will not be able to verify your vote.

These are displayed on the screen in a click-to-open manner, as seen in Figure 8 - Image of the FAQs screen from the IT artefact.

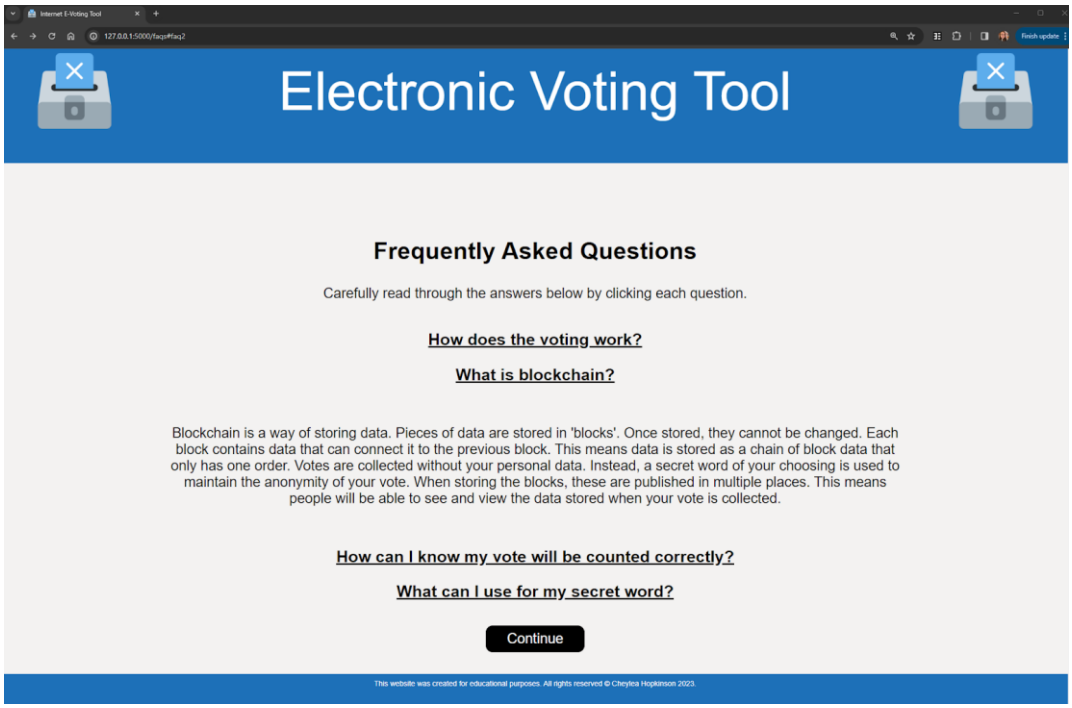

Figure 8 - Image of the FAQs screen from the IT artefact

4.3.2 Check Eligibility

Once the user is happy with the FAQs, they then move on to having their eligibility checked. This occurs before any identification checks occur so that a photo of the users' identity is not collected unnecessarily. An initial screen warns the user that their eligibility is about to be checked.

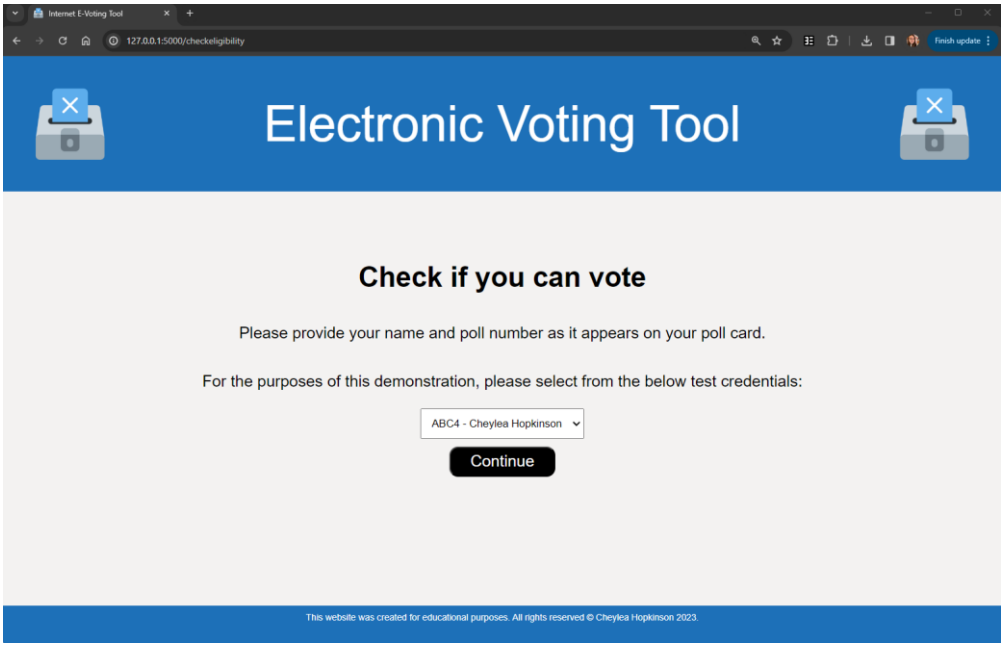

Figure 9 - Image of the Check Eligibility screen from the IT artefact

Below, Figure 10 shows how the database is called to check eligibility. For this version of the tool, the user selects credentials from a drop-down list for testing purposes; in a finalised implementation, this would be where the poll number or name and address is entered. Nevertheless, the process for checking eligibility remains identical.

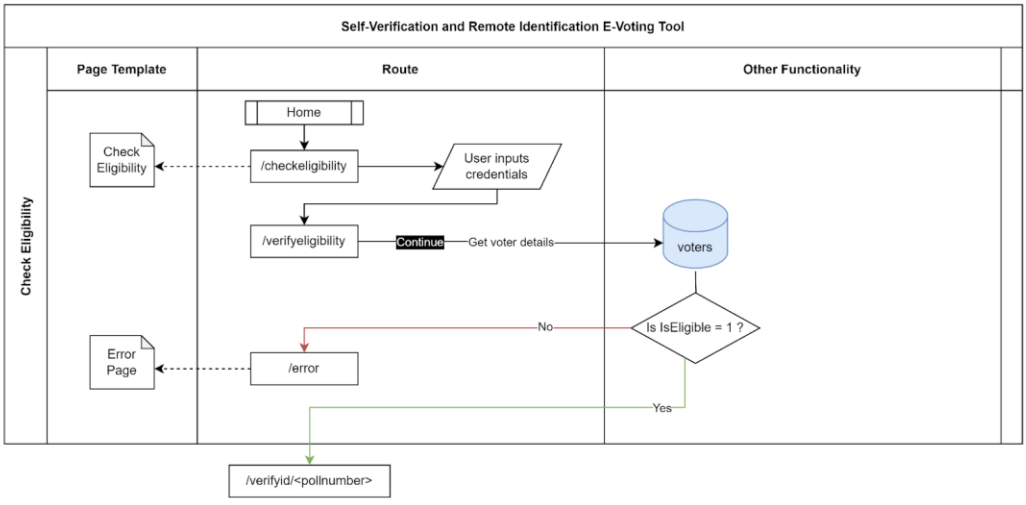

Figure 10 - Diagram to show the workflow for Check Eligibility

Eligibility is determined based on the electoral roll registration (Johnston, 2021) and is pre-loaded into the database at the beginning of the vote. Additionally, once a voter has cast their ballot, they are marked as ineligible to vote again. So, this process can only include those who are still eligible and

have not yet voted to pass this stage. If a user is confirmed as eligible to vote, they can move on to identity verification.

4.3.3 Verify identity (app.py only)

Identity verification starts with a screen that lets the user know they are about to have their identity checked.

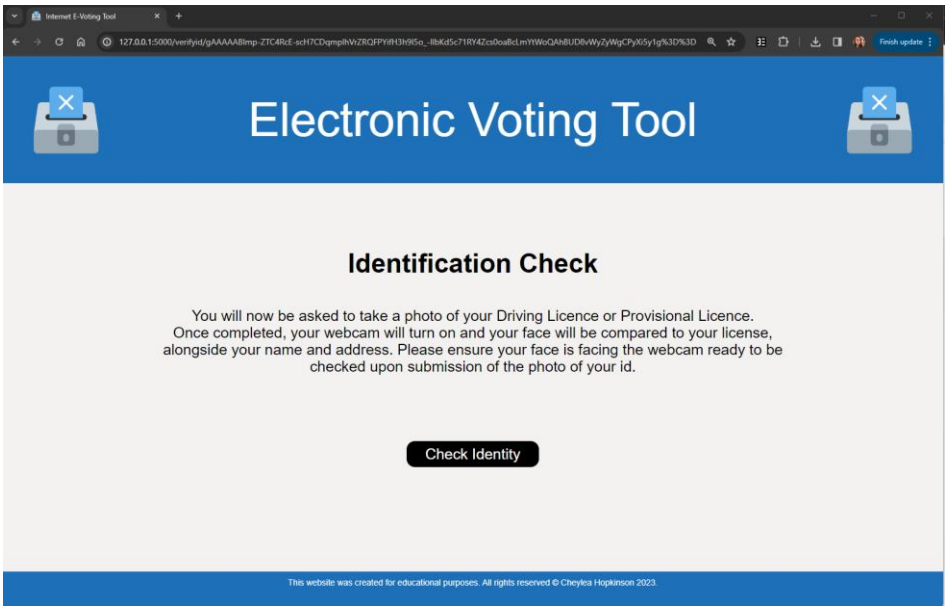

Figure 11 - Image of the Identity Check screen from the IT artefact

The user is warned that they will need their Provisional or Driving Licence and describes how their identity will be checked. In this implementation, the text identification function is only designed to work with these two forms of identification. When clicking '*Check Identity*', the user is taken to a screen where their webcam switches on, and the process to capture an image of their relevant identification begins. Once the image has been captured, the user has the option to try again or proceed with the identity check, as seen in Figure 12.

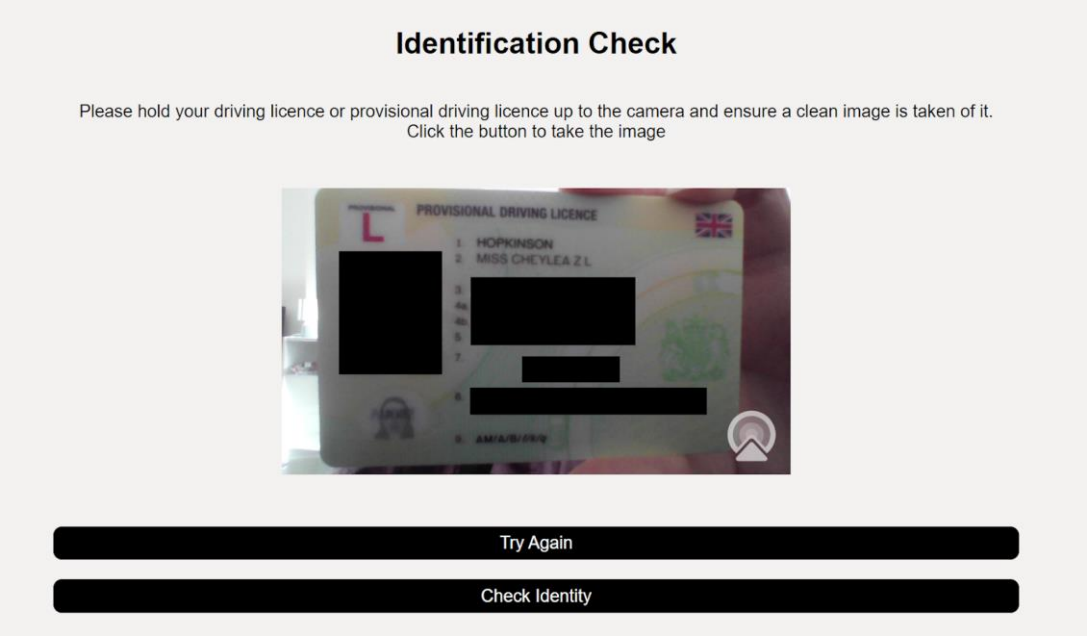

Figure 12 - Image of the Identity Check webcam capture screen from the IT artefact

When "*Check Identity*" is pressed once again, the following steps take place:

- The image is stored temporarily in a folder
- The user's name and address are taken from the database
- The image runs the *check_identification_text* function and checks for similarity between the name and the address. If both have more than 50% similarity, or the name alone has higher than 75%, this is considered a pass for the text check section. If this fails, with similarity scores of below 50%, the process ends, and the user is redirected to the Failure screen. Their image is then deleted.
- If the text identification succeeds, the facial identification commences. This runs the image through the *check_identification_face* function, which opens the webcam to view a live version of the user's face. This is compared to the identity photo found in the image. If a match is found, the person passes. If more than 2 minutes passes without a possible match, this is designated as a failure, and the user is redirected to the Failure screen (see Figure 13). Regardless of the result, the webcam switches off, and the original identity image is deleted.
- The user is redirected to the Pass screen (see Figure 14) if both text and face pass.

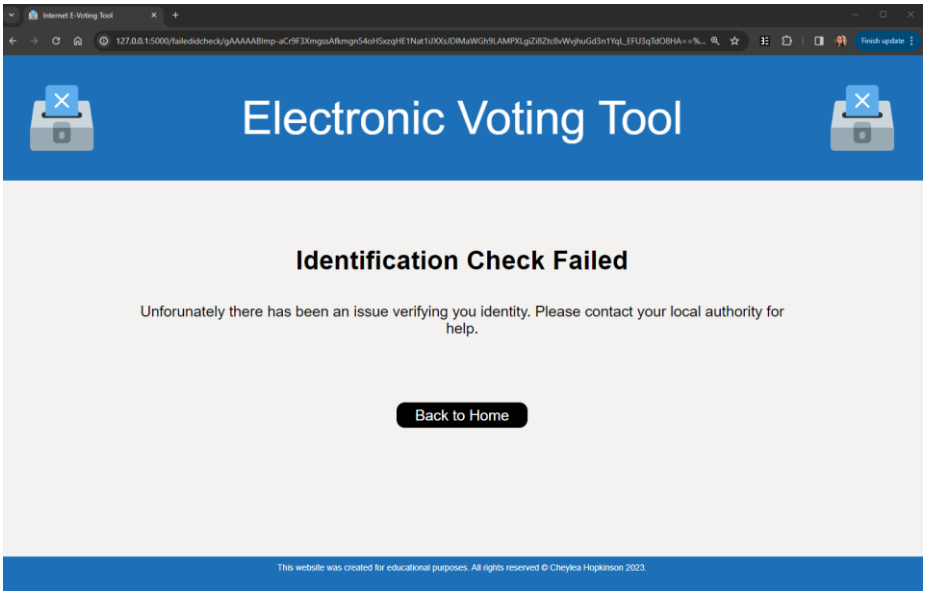

Figure 13 - Image of the Identity Check Failure screen from the IT artefact

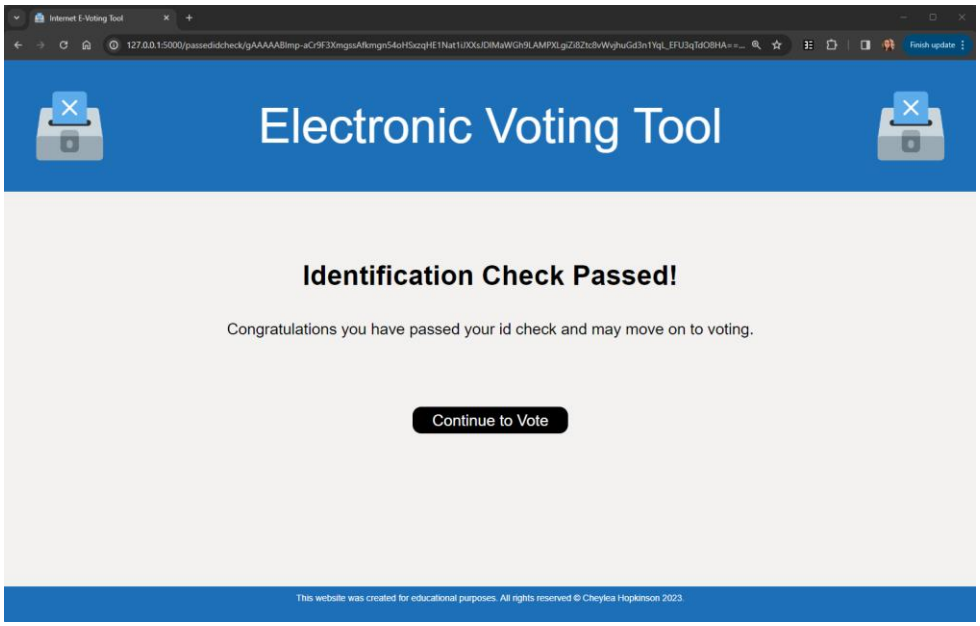

Figure 14 - Image of the Identity Check Pass screen from the IT artefact

In the test version of this tool, workflow went straight from ‘Check Eligibility’ to the ‘Secret Word’ process. A screen would inform the user that this is where the identification check would usually go and prompt the user to continue.

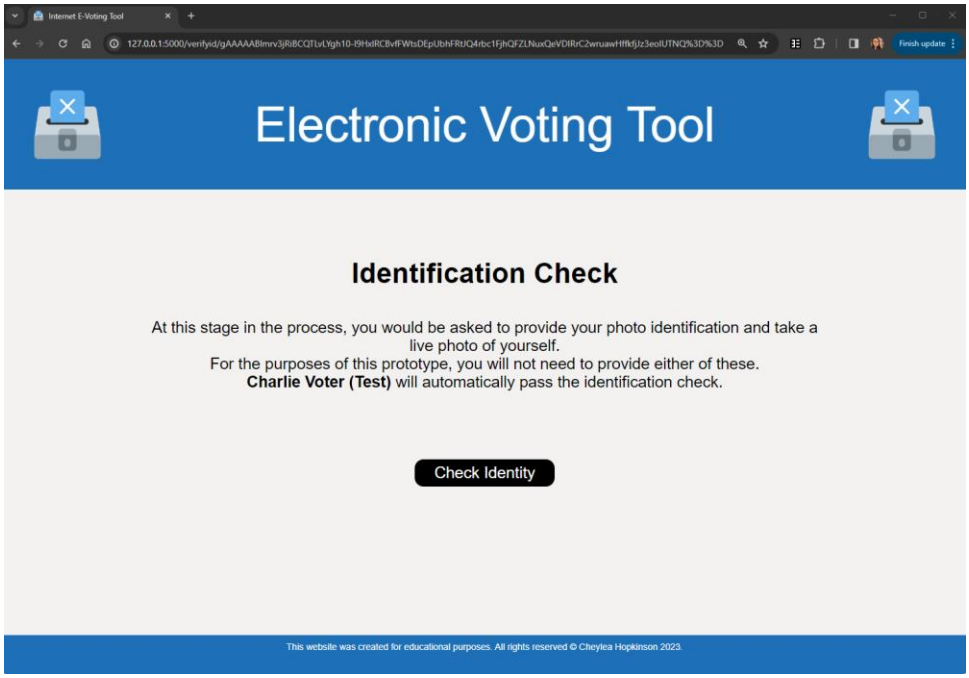

Figure 15 - Image of the Identity Check screen from the test IT artefact

The workflow for this process can be seen in Figure 16.

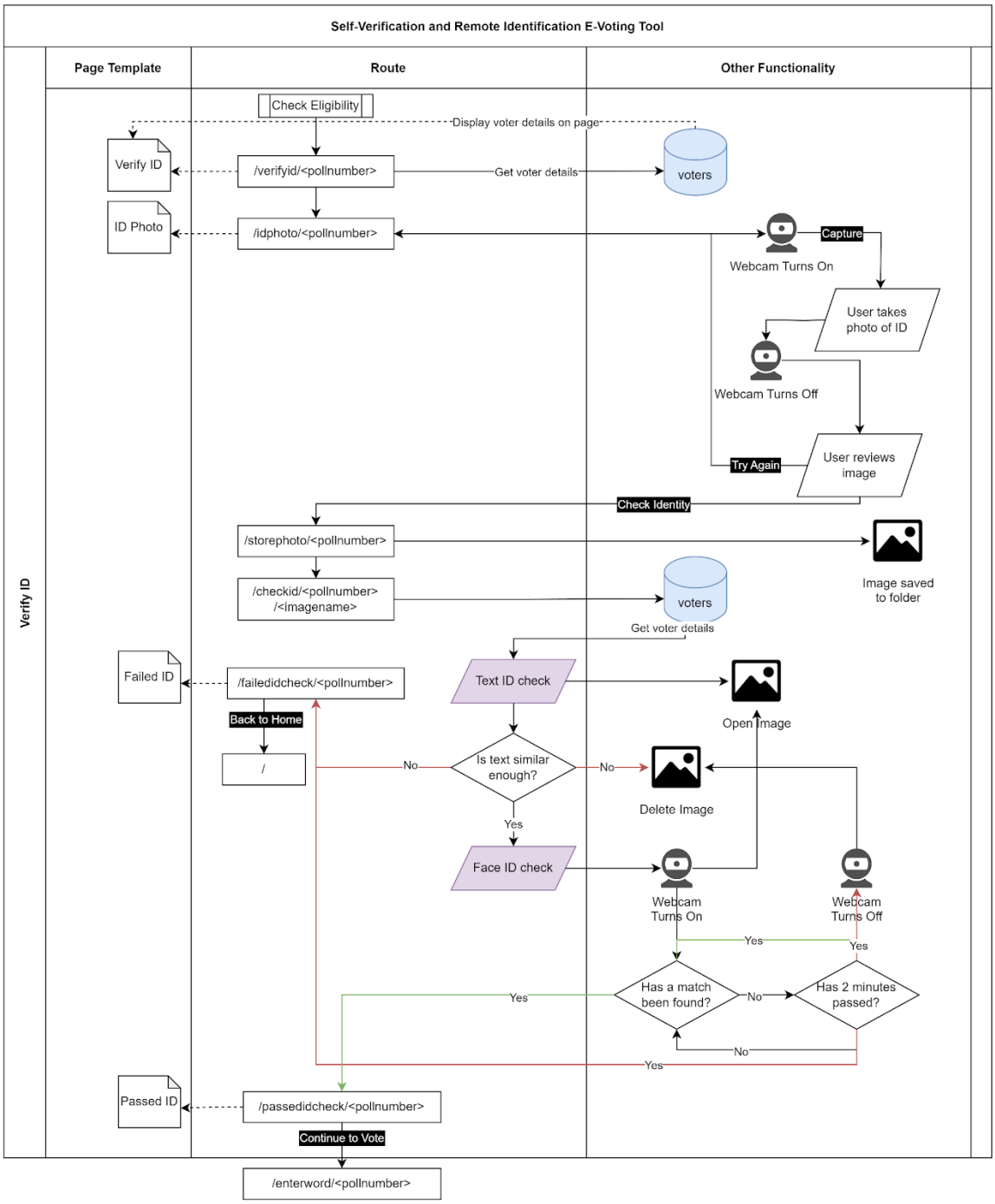

Figure 16 - Diagram to show the workflow for Verify Identity

4.3.4 Secret word

Once the user is confirmed eligible and passed their identity check, they can begin the voting process. This requires first to enter their secret word. If an intended secret word is not allowed, the user can keep

trying until they find one that meets the requirements. There is no need to go through eligibility and identity checks again.

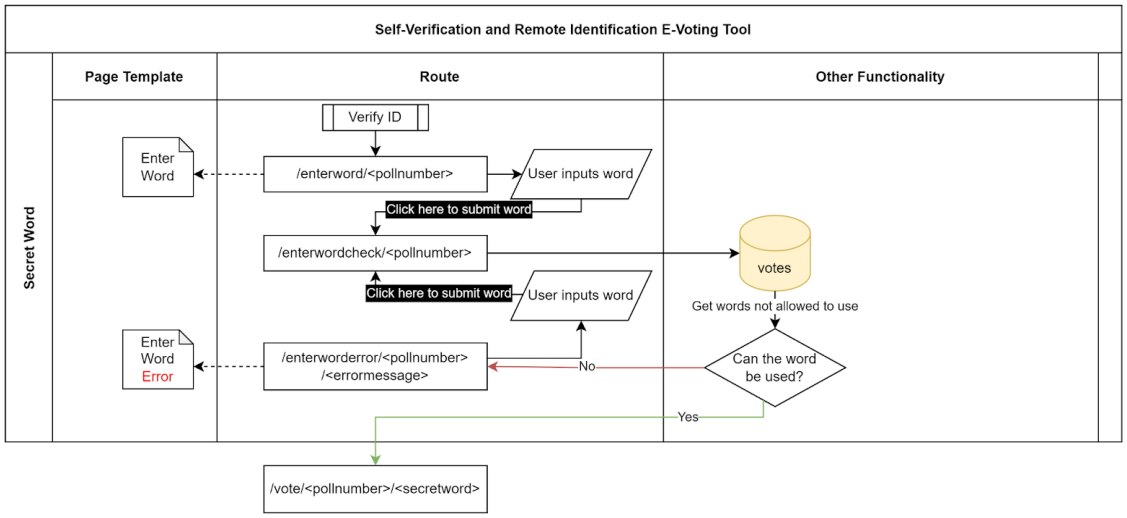

Figure 17 - Diagram to show the workflow for Secret Word

Before the commencement of the vote, the ‘Words’ table will be loaded with words that cannot be used at any poll station, including voters' names and street names. As more words begin to be entered through the election process, these will be added to the table, so that the same secret word cannot be used at the same poll station.

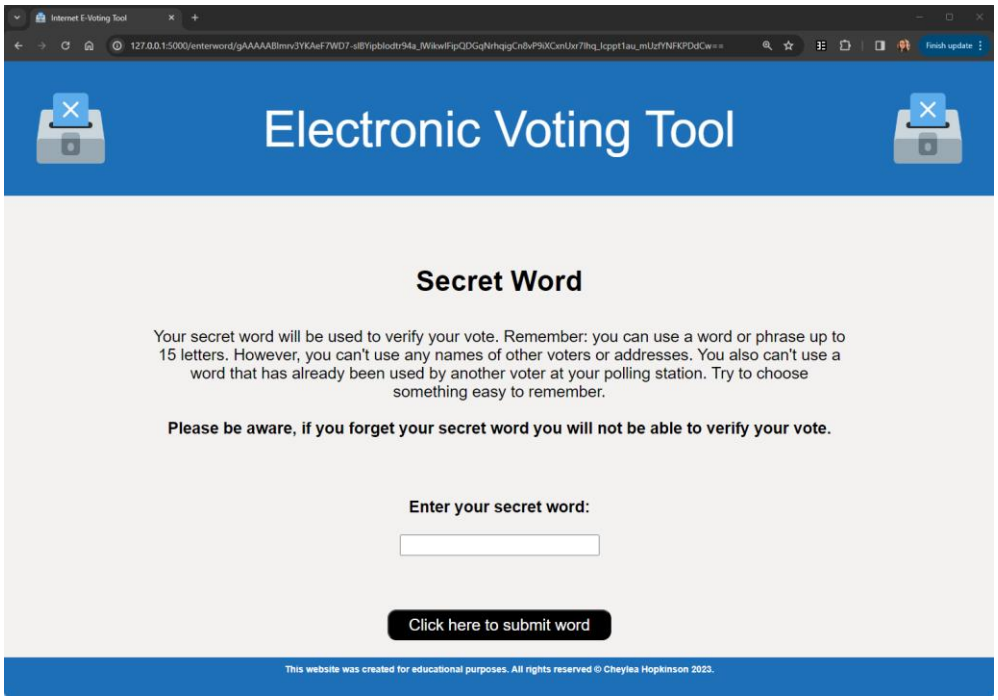

Figure 18 - Image of the Secret Word screen from the IT artefact

4.3.5 Vote

The user can select a candidate to vote when a valid secret word is found. In UK elections, minimal information about the candidates is displayed on the voting slip, which has been recreated here. An extra option is available at the bottom of the screen to account for those who want their vote to count as spoiled.

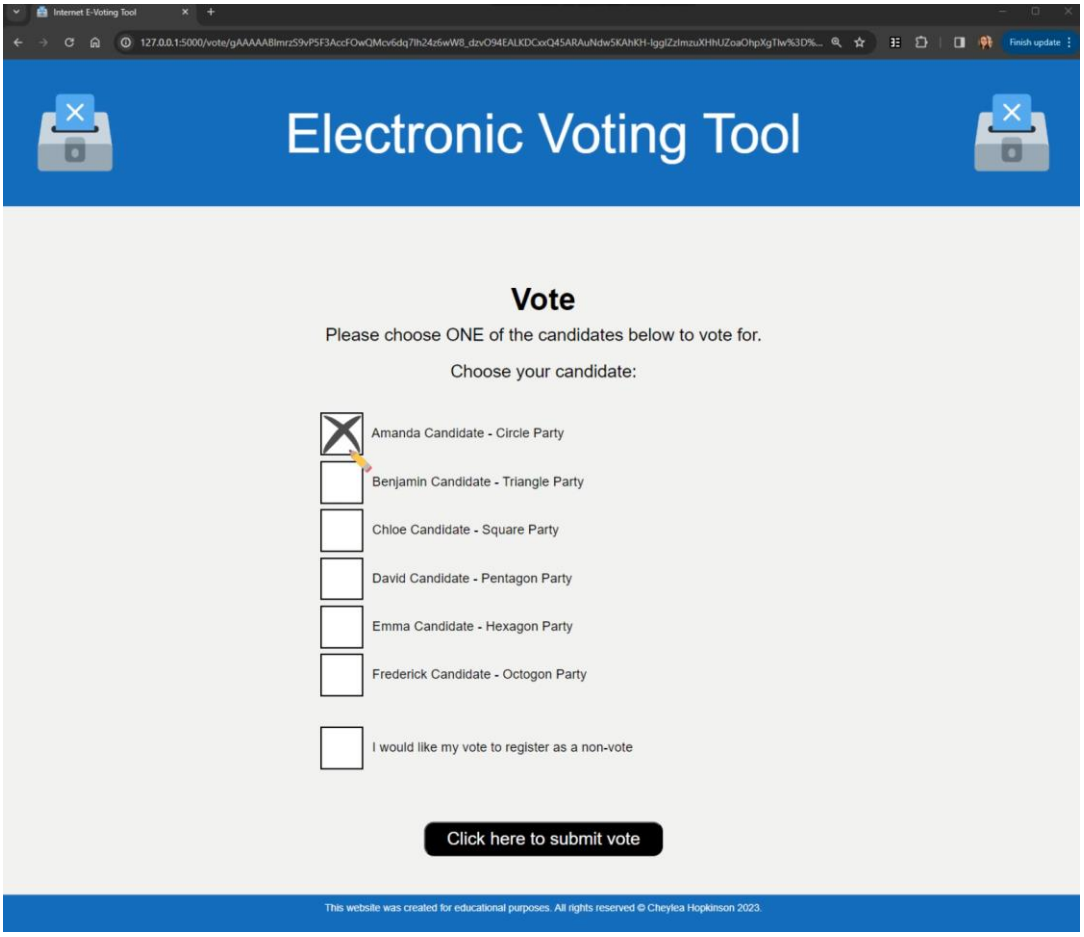

Figure 19 - Image of the Vote screen from the IT artefact

The cursor changes to a pencil when hovering over each option and, when clicked, shows a pencil-like drawing of a cross to mimic voting traditions in the UK. The radio buttons were developed using inspiration from Gavor (2023).

Before the vote is completed, an alert comes on the screen to check that the user is happy with the selected option.

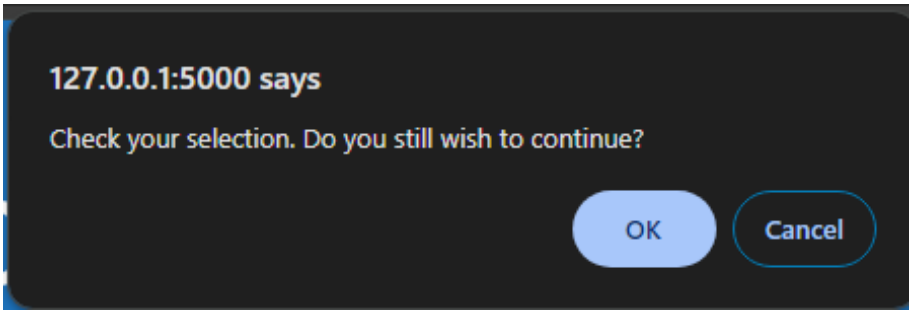

Figure 20 - Image of the alert when confirming to continue with their vote selection

A new vote block is then mined and committed to the 'Votes' database when submitted, as shown in Figure 21.

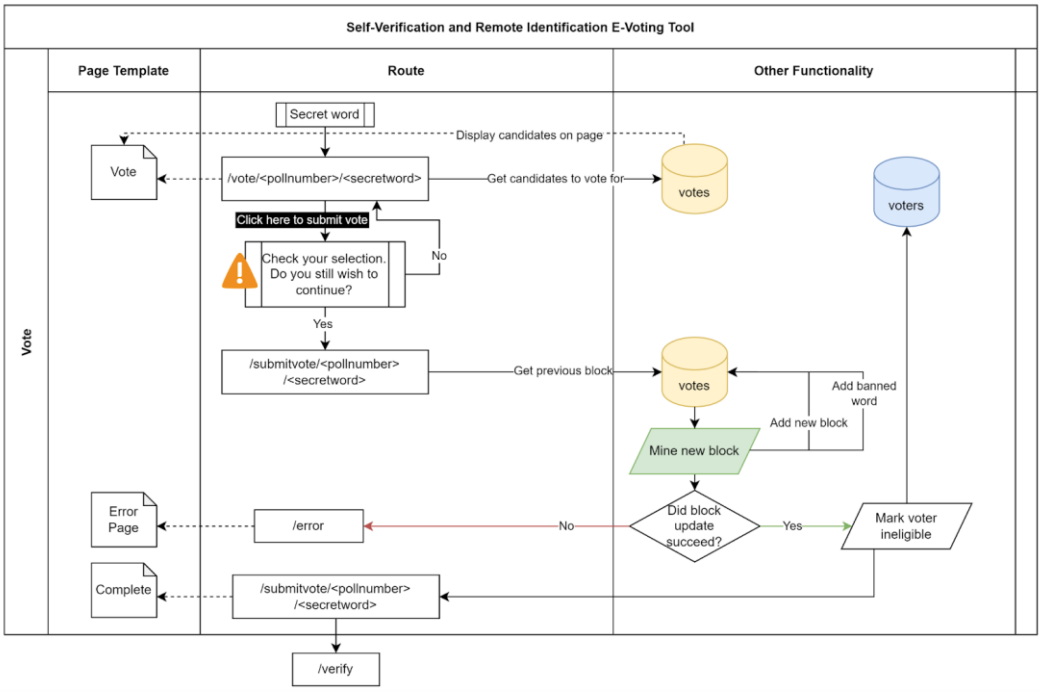

Figure 21 - Diagram to show the workflow for Vote

4.3.6 Verify Vote

At this stage, the user could close the window and never return to the application, and their vote is still counted. However, they have a 5-minute window where they can verify their vote. This can be done immediately, or the user can close the window and return to the verify page within five minutes. To verify their vote, the user enters their secret word and the poll station they voted at. This is then queried from the database and displayed on the screen if valid and 5 minutes have not elapsed.

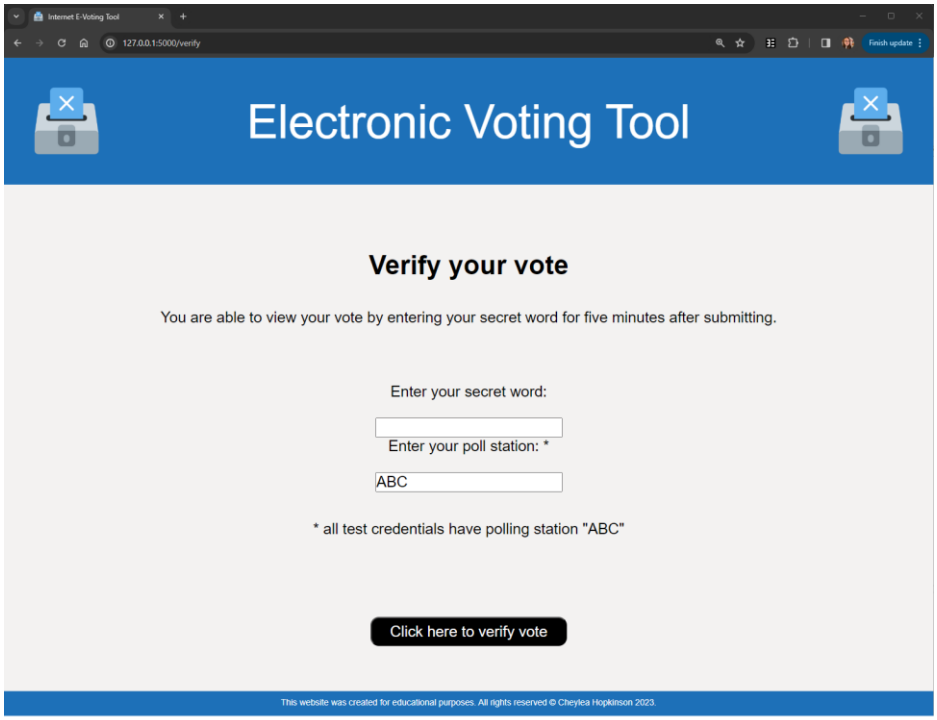

Figure 22 - Image of the Verify Vote screen from the IT artefact

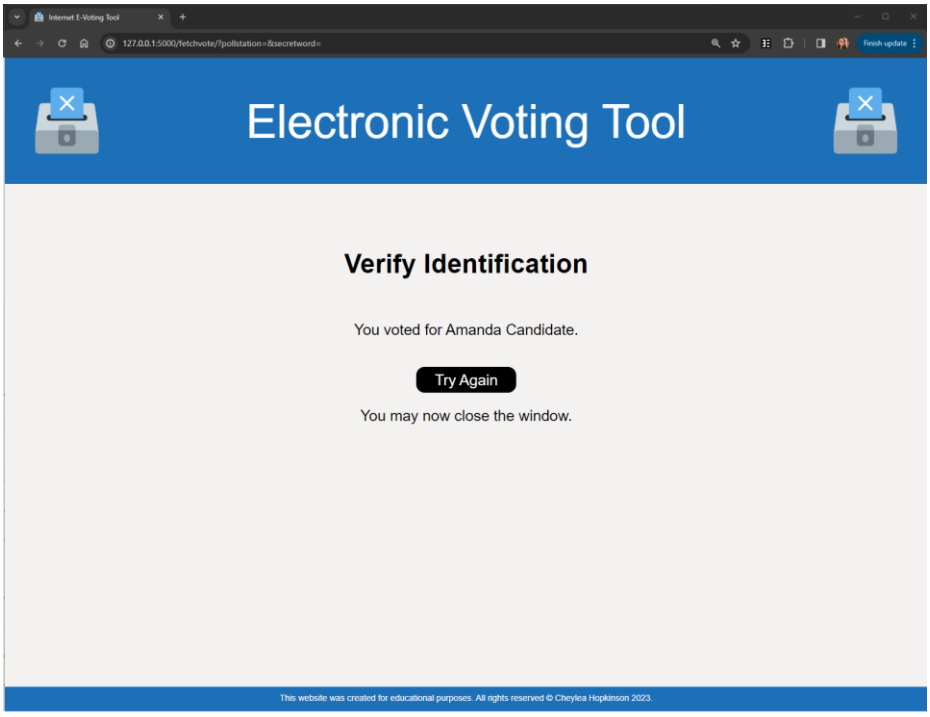

Figure 23 - Image of the Retrieved Vote screen from the IT artefact

Figure 24 shows the final workflow for this verification process.

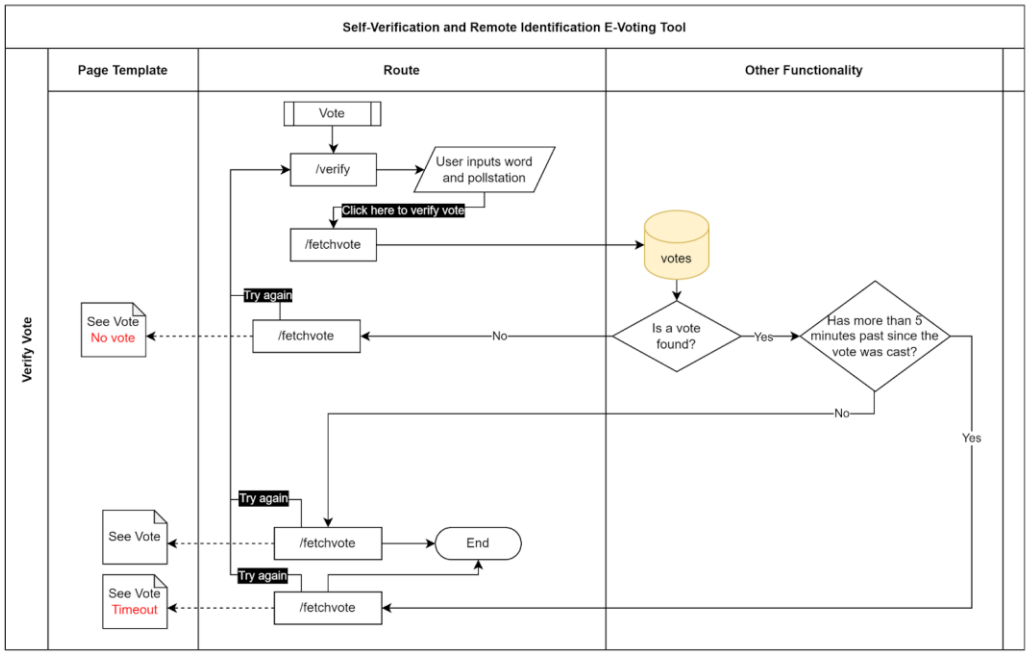

Figure 24 - Diagram to show the workflow for Verify Vote

In the test version of the application, the final screen showed the word ‘CANDIDATE’ to be input as an answer to the relevant screening survey question. This was to check that the respondent legitimately completed the full test of the tool.

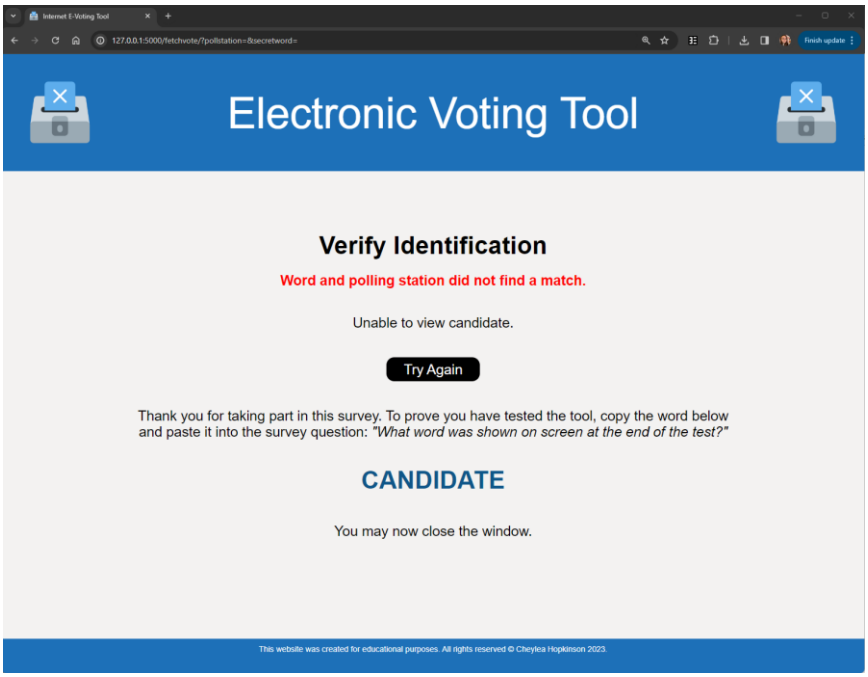

Figure 25 - Image of the Retrieved Vote failure screen from the IT artefact

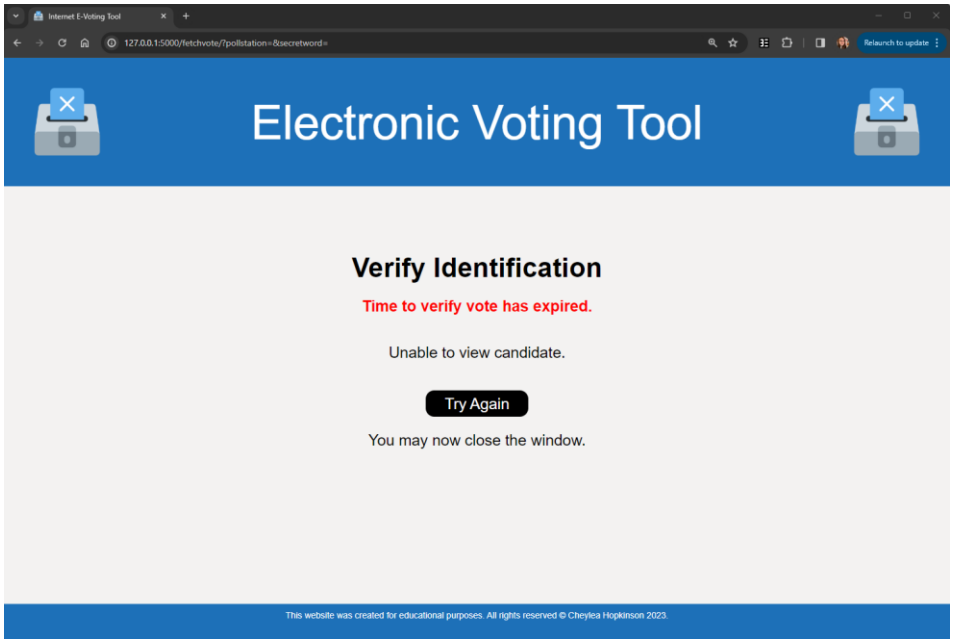

Figure 26 - Image of the Retrieved Vote timeout screen from the IT artefact

Chapter Summary

The produced IT artefact included all required criteria established in the previous chapters. It comprises of a biometric identification element, blockchain vote casting, and the proposed secret word functionality to incorporate verifiability. The implementation followed the original design closely, with only minor amendments, such as the structure of the databases. The development portion of the prototype can be deemed successful. However, the prototype will be further tested in the next chapter to see whether functionality satisfied this project's aims.

Chapter 5. RESULTS AND EVALUATION

5.1 Chapter Introduction

To begin to evaluate the artefact, we must refer to the three hypotheses based on the problem statement questions to begin the evaluation.

$H_{0\text{-}1}$ The e-voting tool can identify a user is who they claim to be.

$H_{0\text{-}2}$ The e-voting tool is entirely secure and cannot be tampered with undetected by the public or the government.

$H_{0\text{-}3}$ Voters trust the e-voting tool.

This chapter will evaluate the IT artefact with these hypotheses in mind and determine their probability with the evidence collected.

5.2 Evaluation of IT Artefact

To evaluate if these hypotheses are true, the analysis is split into two parts:

- the results of back-end tests of the functions
- the results of a voting simulation combined with participant survey results

5.2.1 Back-End Function Tests

This section will look at the different functions used in the back-end of the IT artefact and assess their effectiveness in the context of an election e-voting tool. These include the identity related functions for determining if a person is who they claim to be and the blockchain functions for creating the votes to be recorded.

5.2.1.1 Text Recognition and Facial Recognition

To test the reliability of recognition functions, a test was devised to see how consistently it could read text and faces from an image. The functions were run 100 times for an expected pass and 100 times for an expected failure, using 100 different images of a single provisional licence card. 50 of the images were taken on a high-quality camera and another 50 were taken on a lower quality integrated webcam from a laptop. For the purposes of this report and the results, these are referred to as “good webcam” and “bad webcam”, respectively. The image below shows the difference in quality of the images. Other factors considered when taking the images were a variance in lighting, angle, and distance from the camera. This is to mimic variations on how someone may take an image of their identification.

Figure 27 - ID card taken on "bad webcam" (Left), ID taken on "good webcam" (Right)

The file *identification_test.py* in Appendix 6.7D.2.2 contains the functions for running these tests in bulk and writes the results to a text file for later analysis. The tests work by taking a list of image paths and looping through the identification functions.

For positive tests, the correct details and person behind the webcam were used. For the negative test, the same images were used but with a different name “John Smith”, a similar address and a different person. For text recognition, the pass rate was set to a minimum of 0.75 similarity for the name or 0.5 similarity for both name and address. The results are shown in the tables below:

Text Recognition	Matching Text	Non-Matching Text
Positive	16 (15 good, 1 bad)	84 (35 good, 49 bad)
Negative	0 (0 good, 0 bad)	100 (50 good, 50 bad)

Table 2 - Confusion matric for text recognition function

Function	Sensitivity	Specificity	Accuracy
check_identification_text (all)	100	54	58%
check_identification_text (good)	100	59	65%
check_identification_text (bad)	100	51	51%

Table 3 - Sensitivity, specificity and accuracy results for text identification function

Face Recognition	Matching Face	Non-Matching Face
Positive	95 (50 good, 45 bad)	5 (0 good, 5 bad)
Negative	2 (0 good, 2 bad)	98 (50 good, 48 bad)

Table 4 - Confusion matric for face recognition function

Function	Sensitivity	Specificity	Accuracy
check_identification_face (all)	97.94	95.14	96.5%
check_identification_face (good)	100	100	100%
check_identification_face (bad)	95.7	90.57	93%

Table 5 - Sensitivity, specificity and accuracy results for face identification function

The results demonstrate that for text recognition all positive matches were correct, but around half of the time positive matches are marked false. The bad webcam had slightly worse performance for this. The good webcam images were easier for the text functions to read,with more matches found for expected matches, however, neither were able to return a pass consistently.

For facial recognition, the results show a much higher accuracy compared to the text identification, with only a few images where it struggled to get the right result. Upon review, it was images that had reflective parts or poor lighting that had the most fails. This could be circumvented by giving clearer instructions to the user on how to take a photo of their identity, though the function was still much more effective with the good webcam. What is concerning are the two false positives, which implies that it could be possible for someone to pass when they should not. This could be improved by tweaking the pass parameters and improving the data that drives the facial recognition model.

For both of these features, they are widely used and established technology and there are other models that could be substituted in place of these within the tool design, such as Passport & ID VIZ OCR and Authentication Software, which can read almost all travel document identities (Airport Suppliers, 2023).

5.2.1.2 Blockchain Validity and Verification

This section will test how possible it is to detect if a block has been tampered with. A simulation was run with random interference to simulate 'hacking' of the committed vote block. This involved amending the block after mining and before adding it to the chain. This was achieved by using the *chain_valid* function within the Blockchain class to check the legitimacy of the chain to attempt to detect ones that may have been altered.

The *chain_valid* function works by checking the hash value of the previous block and determining if, when reverse engineered, the hash calculation is in the correct format. This function alongside the other functions from the Blockchain class were created using information from a related Geeks for Geeks (2023) article.

For testing, a function was designed to occasionally add random interference when constructing a chain, as seen in Appendix 6.7D.2.1 . It works by generating a random number, and if below 0.01 it will amend the hash and replace the value of the candidate, meaning some chains will be valid and others will not. For the sake of this test, this added 'HACKED' to the beginning of the hash value, so that altered values can easily be identified. The test function created 200 blockchains of length 20 and used the *chain_valid* function to test if it could detect changes it.

Valid Blockchain	Valid chain	Invalid chain
Positive	161	0
Negative	0	39

Table 6 - Confusion matrix for valid blockchain test

Function	Sensitivity	Specificity	Accuracy
Blockchain()	100	100	100%

Table 7 - Sensitivity, specificity and accuracy results for valid blockchain test

As expected, due to the nature of blockchain, the results had a 100% accuracy. As such, a similar validity check could be run on the vote results in a real scenario and an amended or additional block would be picked up. If the chains were broadcast on the peer-to-peer network, discrepancies could also be detected if there were mismatches. What is not covered in this testing is if a bad actor was able to only replace the candidate value and left the chain intact. This could only be picked up by the self-verification of voters themselves.

5.2.2 Survey Results

The survey fieldwork commenced on the 11th of October until the 18th of December, with 95 responses, of which 84 were valid. The full set of questions asked can be found in 6.7Appendix E. It was conducted using Microsoft Forms and answers were collected anonymously. A response was considered valid if the criteria were met and the screening question answered correctly. The questions and the answers required to be a valid response can be found in the table below.

Are you over the age of 18?	Yes
Have you previously voted in an election in the UK (local or general)?	Yes
What word was shown on screen at the end of the test?	Candidate

Table 8 - Screening question and answers for a valid survey response

The age and voting experience of participants are broken down in Figure 28, with more than half of participants in the 25-39 age bracket and the majority of participants declaring that they usually vote in-person, as opposed to post.

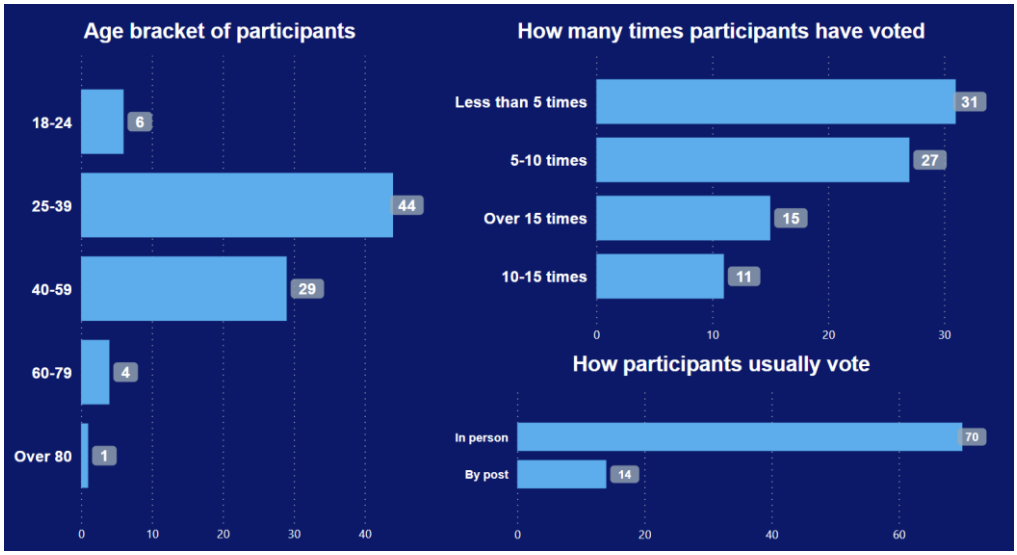

Figure 28 - Demographic breakdown of valid survey responses

5.2.2.1 Impressions of the IT Artefact

Most participants found the tool easy to understand and use, with 94.05% saying it was either 'Extremely easy/clear' or 'Somewhat easy/clear' to understand and use the tool. Having tested the tool, 58.3% (n=49) said they would be more likely to consider electronic voting in the future, with 93.9% (n=46) of this support coming from those aged between 25 and 59.

As described in the survey design, these questions used a Likert scale from "Strongly Agree" to "Strongly Disagree" to capture the level of agreement with the statement (Bhandari and Nikolopoulou, 2022). 56.0% of participants also reported to have a stronger understanding of blockchain. This all suggests the tool is generally easy to use and informative.

The most divisive of questions was that regarding the practice of showing identification before voting. Participants were asked:

Do you agree or disagree with the following statement: The new requirement to show photographic ID at polling stations in the UK to vote is a good thing.

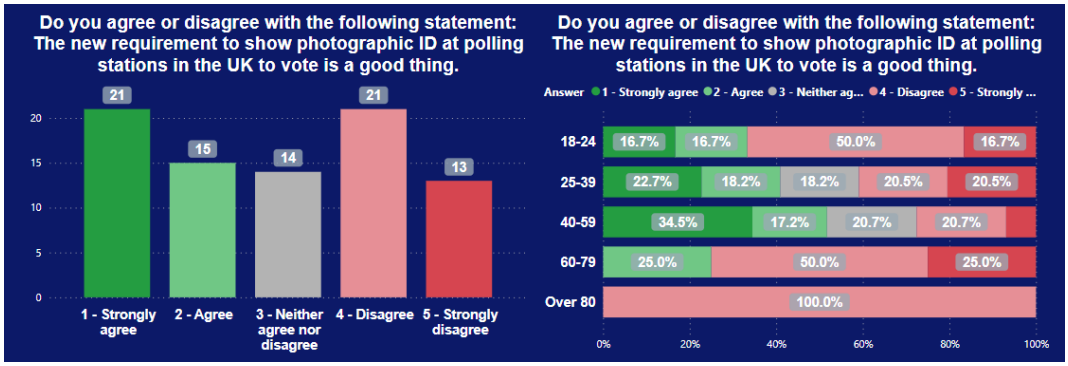

Figure 29 - Graph for answers to "Do you agree or disagree with the following statement: The new requirement to show photographic ID at polling stations in the UK to vote is a good thing."

40.5% (n=34) of participants disagreed with the new requirement, which is consistent across all age groups. However, 65.5% (n=55) still reported they would be comfortable providing a photo of their identification to the voting tool.

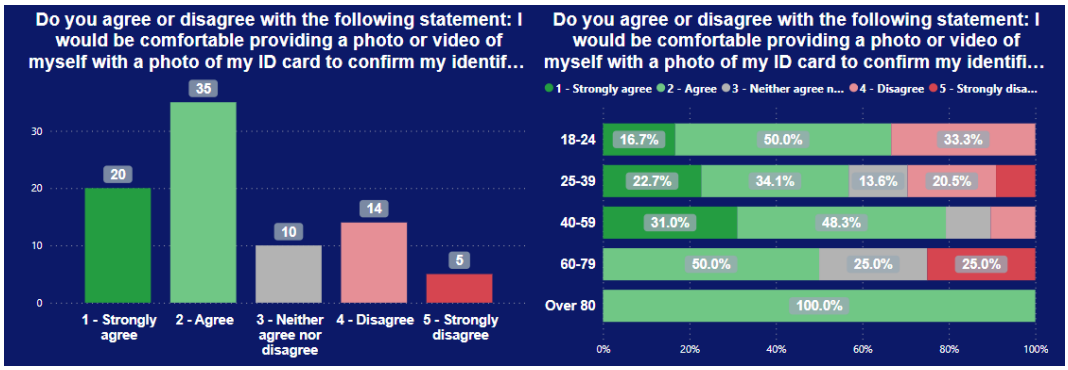

Figure 30 - Graph for answers to "Do you agree or disagree with the following statement: Do you agree or disagree with the following statement: I would be comfortable providing a photo or video of myself with a photo of my ID card to confirm my identification when voting."

In terms of trusting the tool, participants were asked:

Do you agree or disagree with the following statement: I can trust the electronic voting tool to count my vote correctly.

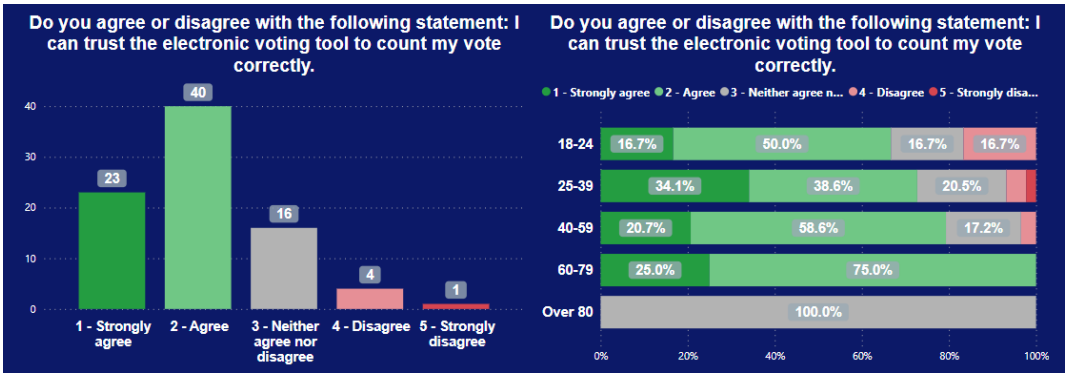

Figure 31 - Graphs for answers to "Do you agree or disagree with the following statement: I can trust the electronic voting tool to count my vote correctly."

Of those who answered, 75.0% (n=63) felt that they could trust the tool to count their vote correctly, with the disagreements sitting more firmly with the younger end of participants.

5.2.2.2 Opinion Analysis of IT Artefact

Participants optionally provided other things they liked or disliked about the tool. The answers were coded into categories to analyse the different topic areas.

Of the participants, 28 gave answers to what they liked, with 21 responses referring to how quick and easy the tool was to use. There was also praise for the option to spoil their ballot, how similar the candidate layout felt to a real vote, and even one participant that specifically stated how they felt the explanations helped them build trust in the tool.

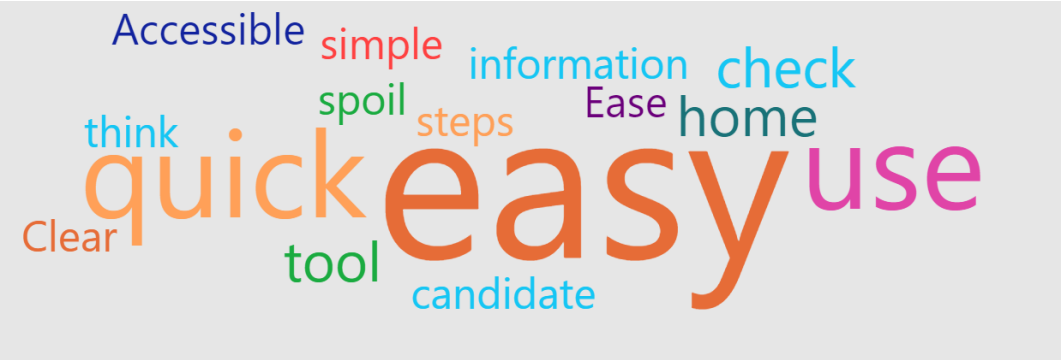

Figure 32 - Word cloud for answers to "Are there any other things you liked about the tool?"

Regarding what participants disliked, there were a total of 26 comments left and below details the main themes:

- **Dislike for Biometric Identification:** 4 participants mention concerns around how the identity process would work, and that being required to produce photo identification during the voting process would hurt voter turnout.

- **Blockchain confusion:** 3 participants reported that they still felt confused about how block-chain would work.

- **Accessibility concerns:** 3 brought up concerns around accessibility and worry that certain people would be unable to complete their vote online.

- **Verification confusion:** 6 participants reference the verification process. Some participants mentioned they think it would be difficult or inconvenient for everyone to think of secret words. Another participant questioned the point of the timeout and why they would not be able to see their vote at any time. The reason for the timeout is not mentioned in the e-voting tool and throughout the survey, there is no comment from any participant on concerns around coercion.

- **User interface improvements:** 5 participants suggested things that could improve the user interface. This included converting the web application tool into a mobile application instead, including security authentications, screen reading and other accessibility options, and adding more candidate information like logos and photos.

5.2.2.3 Understanding E-Voting

Before testing the tool, participants were asked if they had heard of e-voting before and those that had were asked gated questions based on existing knowledge. 71.4% (n=60) of participants had heard of e-voting before, 40.0% (n=24) of whom felt they would be more likely to consider voting if electronic voting was an option. This was especially prominent for 25-39-year-olds, where more than half felt they would be more likely to vote if it was an option.

Prior to testing the tool, participants were asked:

Do you agree or disagree with the following statement: Electronic voting is a good thing that should be used in the UK

The question was asked twice, once to those who had heard of e-voting before testing the tool and once to all after the testing. The opinions of those who answered the first question remained mostly the same, with only 13.3% (n=8) of participants improving their opinion. The concluding result after testing for all participants revealed two-thirds of them felt electronic voting was good for the UK and was not dependent on age.

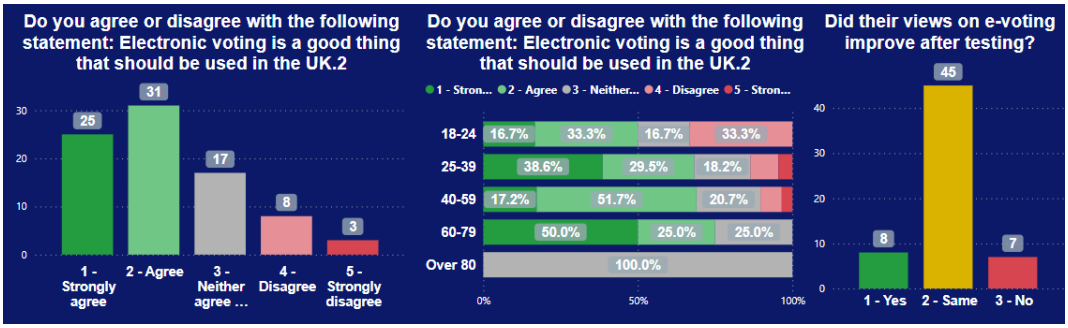

Figure 33 - Graph of answers for "Do you agree or disagree with the following statement: Electronic voting is a good thing that should be used in the UK" that was asked a second time

Participants were asked about their worries for electronic voting, and were able to select as many options as they liked. They were asked again after testing in the context of using the IT artefact. The top three concerns were on keeping their identity safe, wanting more research before implementation, and concerns around data misuse. There were however 16 participants that felt they had no worries or concerns about electronic voting in this context.

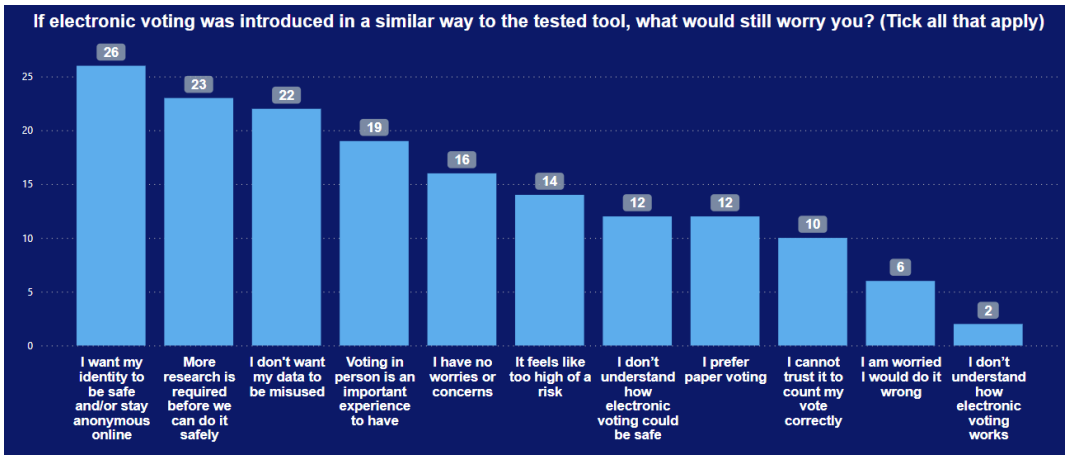

Figure 34 - Graph for answers to "If electronic voting was introduced in a similar way to the tested tool, what would still worry you? (Tick all that apply)"

5.2.2.4 Electronic Voting Opinion Analysis

Participants were asked to describe their main advantage and main drawback for electronic voting in their own words to give them an opportunity to have their own personal say on what they think about electronic voting. These were categorised into common themes to analyse the results.

For main advantages, the top two responses were convenient (30.1%) and easy (25.3%). For main drawbacks, the overwhelming majority highlighted the security of their vote at 45.9%. Accessibility appeared as both an advantage (as it is easier for some people to access things online than in-person) and as a drawback (not everyone has computer literacy or a stable internet connection).

The full breakdown can be seen in the tables below.

Advantages	Total Participants	% Participants
Accessibility	10	12.1%
Accuracy	1	1.2%
Convenient	25	30.1%
Cost Saving	2	2.4%
Easy	21	25.3%
Increased Turnout	8	9.6%
None	4	4.8%
Progressive	1	1.2%
Quick	10	12.1%
Secure	1	1.2%

Table 9 - Table of answers to "What is the one main advantage of electronic voting for you?"

Drawbacks	Total Participants	% Participants
Accessibility	8	9.6%
Data Protection	11	13.3%
Decreased Turnout	2	2.4%
Impersonal	1	1.2%
No paper trail	1	1.2%
None	10	12.1%

Technical Failure	5	6.0%
Too Complex	3	3.6%
Vote not secure	38	45.8%
Voting in person is good for you	2	2.4%
Wrong people voting	2	2.4%

Table 10 - Table of answers to "What is the one main drawback of electronic voting for you?"

5.2.2.5 Survey Simulation

During the survey, users could cast votes successfully, with at least a 92.0% success rate in completing a vote based on those who were able to report the correct word on the final screen. Despite approximately 84 people completing a vote, close to 200 votes were cast in the database. This is likely due to resubmission on the page by going back and forth or refreshing. This could be amended by preventing duplicate words at this stage instead of an earlier page or another feature preventing form resubmission.

5.2.2.6 Survey Summary

The results show that for those who participated the majority of responses felt the tool was quick and easy to use. The sample in this survey is small but could be scaled to a wider audience to improve the accuracy. The verifiability process worked successfully which indicates votes are being recorded accurately. Opinions on electronic voting and the results from the trust-based question show an overall positive public opinion on e-voting and some potential in the concept of the tool. Since the survey has a small sample size, we can use The Wilson Confidence Interval (Franco et al., 2019) to determine that, if this research is repeated, the proportion of people who would trust the tool to count their vote correctly would be between 66% and 84%. For those who think electronic voting would be a good thing, this would sit between 56% and 76%. These results show promising levels of agreeability.

5.3 Chapter Summary

The chapter explores the different data gathered by the evaluation tests. The artefact was given criteria that it must meet to be successful, and the results for this are summarised below.

- **Verifiable votes that do not jeopardise privacy or risk coercion:** The survey participants were able verify their votes during the vote simulation successfully without a risk to their privacy. Coercion was not raised by any participant as a concern during the survey, although this was not a focus of the survey questions.

- **An ID system that prevents voter fraud but keeps anonymity safe:** A simulation to assess the identification was run and both face and text worked successfully, meaning it is possible for the tool to identify if a user if who they claim. The ID images do not require long term storage to preserve anonymity. The results did, however, show differing level of consistency, including 2 false positives when using a poor-quality webcam. The webcam image's quality also heavily impacted the text recognition results, and it cannot be expected that every adult will have access to a high-quality camera. This would need to be rectified to truly prevent all voter fraud.

- **Votes are secure, accurately recorded and the count of votes can be proven:** The simulation for invalid blockchains demonstrated how amended chains could be detected, and the blockchain technology used in the tool could be scaled up with confidence.

- **The tool is accessible to potential voters:** The survey results showed an overwhelming response for how easy and convenient the tool was to use. There were some concerns raised around the accessibility for all, with calls for an improved user interface and questions as to whether those with a stable internet connection and computer literacy would be able to vote.

Henceforth, the tool successfully meets the majority of the criteria. With this in mind, we can review the problem statement questions.

1. **Can an internet e-voting system identification check be remote whilst ensuring accuracy and voter anonymity?**

Yes - the artefact was successfully able to perform identity checks accurately and does not store sensitive information for extended periods of time.

2. **Would an internet e-voting system compromise the security of the vote casting?**

No – any changes to the blocks would be identified using chain validity detection function and the peer-to-peer blockchain network for tampering with votes in storage. For votes that could be tampered with in transit, self-verification when checking their vote would detect the changes.

3. **Can an internet e-voting system provide two-way transparency between voters and the governing body?**

Yes, with limitations – the survey results show that there is potential for a positive reception to the e-voting tool and electronic voting in general, but this is distant from a fully trusted system.

The next chapter will discuss the conclusions of these findings.

Chapter 6. CONCLUSIONS

6.1 Chapter Introduction

This project has explored many areas of electronic voting and how it could be executed in the UK. To further the research, a prototype internet e-voting tool was created with features including identification, secure voting storage, and a verification method designed to be easier to understand while remaining receipt-free. The questions and hypotheses proposed in this body of work have been evaluated using the designed tool in many different ways to determine their answers. This conclusion will collate all of those findings and discuss the strengths, weaknesses and areas that require further development.

6.2 Lessons Learned

There are many subjectivities to defining what an effective voting system requires. The system needs to be air-tight, and the average person must trust that their vote will be counted as they want.

The limitations of traditional paper voting ballots are well documented, but its most significant advantage is its simplicity: you mark a paper, and someone counts it under supervision. There are thousands of polling stations all over the country. It is difficult for any third party to tamper or affect the voting process on such a large scale, as it requires reaching many individuals in many rooms. Solutions that involve internet connectivity mean a bad actor only needs to find one successful access point to change votes at scale. Blockchain has the potential to bridge that gap. Still, when misunderstood, it is a complex technology that could doubt the integrity of elections and their results, even if the security design is nearly flawless.

To summarise, as much as this is a technology and security problem, it is also a human one, and this must at least be considered in subsequent research in this field.

6.3 Strengths and Weakness of the Project

The results in chapter five show that creating a voting solution with an identity check and secure storage and verification would be acceptable to most of the UK population A fifth of the UK population is not satisfied with the current election voting process (Electoral Commission, 2023c), and this research shows it is at least possible for people to consider something like the internet e-voting tool to vote. Technologically, storing data in a blockchain that can be broadcast to many places in a decentralised manner would enable quick verification of the results on a large scale; with a voter self-verification system that satisfies user verifiability. Although not without limitations in this implementation, online identification software is continually being developed and improved for other secure environments, like banking applications.

Considering the hypotheses, we can confirm that the e-voting tool can identify whether a user is who they claim to be. Although we cannot fully determine if the blockchain system in the e-voting tool is entirely secure, we have shown that tampering can be detectable. And finally, the results from the survey show an easy-to-use tool that, in turn, was rated as trustable by 75% of participants.

However, considering the survey results, the number of participants is small, and an online survey may be biased toward those already comfortable in an online space. A few participants, including one over 80, described how computers and technology were difficult to understand. In the UK, 16% of people cannot complete an online application, and 21% of adults do not have all five basic digital skills (Lloyds Bank, 2018). Paper voting does not require these skills. The complexity of technology required to create electronic voting compared to the simplicity of paper may always be a hurdle to those who struggle with technology. Additionally, self-reported understanding and trust during testing may be relevant, but do not consider possible attempts to cast doubt on the voting software and how it works before an election. Further research on capturing and maintaining trust would be the key to successfully implementing internet e-voting in the UK.

A gap in consideration in this project is that if a vote is altered in transit, self-verification is the sole function of detection. This then begs the question: what would be the process if a voter needed to report their vote is incorrect? Is it possible for a bad actor to specifically target those who would not take the time? And if the system can be designed such that a vote simply cannot be interfered with, and self-

verification is just for peace of mind - what if it is lied about, and how would that jeopardise the trust in the system? In this case, we appear to have an acceptable hypothesis that tampering can be detected, but how to deal with the consequences of this has not been explored. Additionally, considering coercion, it would still be possible for a voter to pass the ID check and then be forced to vote in a certain way.

Finally, there is a distinct gap in evaluating how effectively the secret word verification system would prevent coercion. This was not explicitly asked in the survey. Although identity verification would prevent external electoral fraud, it is still possible for those familiar with the voter to influence and intercept their vote. The possibility of this in paper voting is limited, as once identification takes place, the person will go alone to the booth to vote privately (assuming disability or mobility help is not required).

6.4 Academic Application and Limitations

From an academic perspective, the prototype was limited to a blockchain network on a conceptual level, but this does not limit the results findings as blockchain is a well-established technology. The facial and text recognition software included in the prototype could also be improved, but similarly this is a well-researched field known to have other working models.

The academic contribution this project brings is through the further exploration of how members of the public feel about e-voting and examining what barriers remain to establish their trust in this system. This paper collates from existing sources what attributes need to be present to move towards trust in an e-voting tool, and the initial survey is a starting point for further research with more resources. This research could be continued to be developed in the areas this study could not cover, such as user testing prototypes with a realised identification technology and gauging the reaction to testers. Another areas of consideration would be to survey for feedback on thoughts if both paper voting and e-voting were run simultaneously.

6.5 Business Application and Limitations

The artefact design could be adapted to create a product used for online voting that requires an identification check and strong verification. Although this research is limited to statutes around government

elections in the UK, this research could be applied to other countries and other purposes for e-voting. There are many NGOs that this could be piloted that require a secure voting process, an example would be universities for board members or student elections. The possibilities are vast.

This research also proves how blockchain technology can successfully integrate with identification checking to create a use case to handle sensitive information. Any enterprise that would find value in this relationship can start to harness blockchain, whether part of an e-voting tool or separated into proprietary solutions.

6.6 Recommendations / Prospects for Future Research / Work

To continue this ongoing research, more combinations and applications should be tested on broader groups of the UK public to test the level of understanding and trust. These results will iteratively create a model that moves closer and closer to satisfying the hypothesis 'voter's trust the e-voting system.' Additionally, research from the angle of implementing e-voting alongside paper voting, as in Estonia, would be beneficial to see if participants might be more accepting if both options were available to them.

Future research is recommended to conduct evaluations using a scaled-up number of participants. A survey with a sample closer to 400 would give a better confidence level in the results and smooth out the volatility of opinions we saw in some demographics. Research on this scale would require local council or larger NGOs to help pilot the software, in an environment with lower stakes, limiting potential risk factors.

This must be completed alongside the strengthening of biometric identification technology and the security of electronic votes that will keep up with bad actors' continual development of counterattacks and workarounds. It could be possible to find an end-to-end voting system that can be safely used in the UK, but we are not there yet.

6.7 Chapter Summary

The original problem statement examined areas of e-voting that must be upheld for any given e-voting system to be a viable option for the UK to undertake. The IT artefact successfully incorporated a process for remotely identifying individuals, allows votes to be stored using blockchain and allows voters to verify their votes.

The scope of the project seemed just as daunting as the possible scale of its implications in a modernising democracy, but the results show some indication that there may be a solution in the future. Contributing to a body of research that attempts to enshrine transparency, voter representation, and security has been both rewarding and challenging. But, as valued as academic progress in this field may be, polling stations (and thankfully the cute dogs outside them) remain.

REFERENCES CITED

Abuidris, Y., Hassan, A., Hadabi, A. and Elfadul, I. (2019). *Risks and Opportunities of Blockchain Based on E-Voting Systems*. IEEE Xplore. doi:https://doi.org/10.1109/ICCWAMTIP47768.2019.9067529.

Ahsan, A. (2019). Coercion-Resistant E-Voting Scheme with Blind Signatures. *2019 Cybersecurity and Cyber-forensics Conference (CCC)*. doi:https://doi.org/10.1109/ccc.2019.00009.

Airport Suppliers (2023). *Passport & ID VIZ OCR and Authentication Software*. Airport Suppliers. Available at: https://www.airport-suppliers.com/product/passport-id-viz-ocr-and-authentication-software/ (Accessed: 15 Jan. 2024).

BBC News (2011). Vote 2011: UK rejects alternative vote. *BBC News*. 7 May. Available at: https://www.bbc.co.uk/news/uk-politics-13297573 (Accessed: 12 Jan. 2024).

BBC News (2019). General election 2019: What happens at the counts? *BBC News*. 12 Dec. Available at: https://www.bbc.co.uk/news/election-2019-50519374 (Accessed: 14 Jan. 2024).

Belam, M. (2017). *Is it illegal to take a selfie while voting in a polling station?* the Guardian. Available at: https://www.theguardian.com/politics/2017/jun/08/is-it-illegal-to-take-a-selfie-while-voting-in-a-polling-station (Accessed: 27 Dec. 2023).

Bhandari, P. and Nikolopoulou, K. (2022). *Designing and Analysing a Likert Scale | Guide & Examples*. Scribbr. Available at: https://www.scribbr.co.uk/research-methods/likert-scales/ (Accessed: 13 Jan. 2024).

BIJU's Future School (2021). *What is HTML? What are the Benefits, Uses, and Features of HTML in the Real World?* BYJU'S Future School Blog. Available at: https://www.byjusfutureschool.com/blog/what-is-html-what-are-the-benefits-uses-features-of-html-in-real-world/ (Accessed: 5 Jan. 2024).

Birmingham City Council (2023). *Electoral fraud*. www.birmingham.gov.uk. Available at: https://www.birmingham.gov.uk/info/20097/elections_and_voting/983/electoral_fraud (Accessed: 10 Jan. 2024).

Bräunlich, K. and Grimm, R. (2011). Formalization of Receipt-Freeness in the Context of Electronic Voting. *2011 Sixth International Conference on Availability, Reliability and Security*. doi:https://doi.org/10.1109/ares.2011.25.

Chikioke-Keme, K. (2019). *Nigeria is not ready for electronic voting*. www.stears.co. Available at: https://www.stears.co/article/nigeria-is-not-ready-for-electronic-voting/ (Accessed: 29 Jul. 2023).

Davies, N. (2023). *5 benefits of online ID document verification in a digital age*. NorthRow. Available at: https://www.northrow.com/blog/5-benefits-of-online-id-document-verification-in-a-digital-age (Accessed: 15 Jan. 2024).

Denis González, C., Frias Mena, D., Massó Muñoz, A., Rojas, O. and Sosa-Gómez, G. (2022). Electronic Voting System Using an Enterprise Blockchain. *Applied Sciences*, 12(2), p.531. doi:https://doi.org/10.3390/app12020531.

Drake, F.L. (2024). *difflib — Helpers for computing deltas — Python 3.9.2 documentation*. docs.python.org. Available at: https://docs.python.org/3/library/difflib.html (Accessed: 11 Jan. 2024).

Durkin, M. and White, I. (2007). *General Election Dates 1832-2005*. *UK Parliament House of Commons Library*. Available at: https://researchbriefings.files.parliament.uk/documents/SN04512/SN04512.pdf (Accessed: 29 Nov. 2021).

Ehin, P., Solvak, M., Willemson, J. and Vinkel, P. (2022). Internet voting in Estonia 2005–2019: Evidence from eleven elections. *Government Information Quarterly*, 39(4), p.101718. doi:https://doi.org/10.1016/j.giq.2022.101718.

ElectionBuddy (2022). *The Advantages And Disadvantages Of Online Voting Systems*. ElectionBuddy. Available at: https://electionbuddy.com/blog/2022/04/20/the-advantages-and-disadvantages-of-online-voting-systems/ (Accessed: 27 Dec. 2023).

Electoral Commission (2023a). *A guide to polling day - information for media use | Electoral Commission*. www.electoralcommission.org.uk. Available at: https://www.electoralcommission.org.uk/news-and-views/media-centre/a-guide-polling-day-information-media-use (Accessed: 14 Jan. 2024).

Electoral Commission (2023b). *Ensuring that voting is accessible | Electoral Commission*. www.electoralcommission.org.uk. Available at: https://www.electoralcommission.org.uk/guidance-returning-officers-assistance-voting-disabled-voters/ensuring-voting-accessible (Accessed: 14 Jan. 2024).

Electoral Commission (2023c). *Public attitudes 2023 | Electoral Commission*. www.electoralcommission.org.uk. Available at: https://www.electoralcommission.org.uk/research-reports-and-data/public-attitudes/public-attitudes-2023 (Accessed: 8 Jan. 2024).

Engage, U.K. (2018). *Internet voting: Assessing accessibility in elections in the UK*. UK Engage. Available at: https://uk-engage.org/2018/04/accessibility-in-elections/ (Accessed: 27 Dec. 2023).

Faruk, J.H., Islam, M., Alam, F., Shahriar, H. and Rahman, A. (2022). BieVote: A Biometric Identification Enabled Blockchain-Based Secure and Transparent Voting Framework . *Fourth International Conference on Blockchain Computing and Applications (BCCA)*.

Fisher, C. (2019). *What is spoiling your ballot, and how do you do it?* Voting Counts. Available at: https://votingcounts.org.uk/spoilt-ballot.

Franco, C., Little, R.J.A., Louis, T.A. and Slud, E.V. (2019). Comparative Study of Confidence Intervals for Proportions in Complex Sample Surveys†. *Journal of Survey Statistics and Methodology*, 7(3), pp.334–364. doi:https://doi.org/10.1093/jssam/smy019.

Frankenfield, J. (2019). *Hash Definition*. Investopedia. Available at: https://www.investopedia.com/terms/h/hash.asp.

Gavor, D. (2023). *Styling Radio Buttons with CSS (59 Custom Examples)*. Slider Revolution. Available at: https://www.sliderrevolution.com/resources/styling-radio-buttons/ (Accessed: 1 Oct. 2023).

Geeks for Geeks (2023). *Create simple Blockchain using Python*. GeeksforGeeks. Available at: https://www.geeksforgeeks.org/create-simple-blockchain-using-python/ (Accessed: 10 Oct. 2023).

Geitgey, A. (2020). *face-recognition: Recognize faces from Python or from the command line*. PyPI. Available at: https://pypi.org/project/face-recognition/ (Accessed: 11 Jan. 2024).

GOV.UK (n.d.). *Print Types of election, referendums, and who can vote: Overview - GOV.UK*. www.gov.uk. Available at: https://www.gov.uk/elections-in-the-uk/print (Accessed: 1 Jan. 2024).

Hao, F., Wang, S., Bag, S., Procter, R., Shahandashti, S.F., Mehrnezhad, M., Toreini, E., Metere, R. and Liu, L. (2020). End-to-End Verifiable E-Voting Trial for Polling Station Voting. *IEEE Security & Privacy*. doi:https://doi.org/10.1109/msec.2020.3002728.

Hayes, A. (2023). *Blockchain Facts: What Is It, How It Works, and How It Can Be Used*. Investopedia. Available at: https://www.investopedia.com/terms/b/blockchain.asp (Accessed: 27 Dec. 2023).

HM Government (2018). *The Costs of the 2015 UK Parliamentary General Election*. Available at: https://assets.publishing.service.gov.uk/media/5b1e95cf40f0b634d557afc6/The_Costs_of_the_2015_UK_Parliamentary_General_Election.pdf (Accessed: 5 Jan. 2024).

Jafar, U., Aziz, M.J.A. and Shukur, Z. (2021). Blockchain for Electronic Voting System—Review and Open Research Challenges. *Sensors*, 21(17), p.5874. doi:https://doi.org/10.3390/s21175874.

Johnson, H. (2023). *FactCheck: Why will voter identification be required for elections in Great Britain and what ID will polling stations accept – explained*. Channel 4 News. Available at: https://www.channel4.com/news/factcheck/factcheck-why-will-voter-identification-be-required-for-elections-in-great-britain-and-what-id-will-polling-stations-accept-explained.

Johnston, N. (2021). Who can vote in UK elections? *commonslibrary.parliament.uk*. Available at: https://commonslibrary.parliament.uk/research-briefings/cbp-8985/.

Krimmer, R., Duenas-Cid, D. and Krivonosova, I. (2020). Debate: safeguarding democracy during pandemics. Social distancing, postal, or internet voting—the good, the bad or the ugly? *Public Money & Management*, pp.1–3. doi:https://doi.org/10.1080/09540962.2020.1766222.

Lake, J. (2023). *What is fernet and when should you use it?* Comparitech.com. Available at: https://www.comparitech.com/blog/information-security/what-is-fernet/ (Accessed: 13 Jan. 2024).

Lee, M. (2023). *pytesseract: Python-tesseract is a python wrapper for Google's Tesseract-OCR*. PyPI. Available at: https://pypi.org/project/pytesseract/.

Lloyds Bank (2018). *UK Consumer Digital Index 2018*. Available at: https://www.lloydsbank.com/assets/media/pdfs/banking_with_us/whats-happening/LB-Consumer-Digital-Index-2018-Report.pdf (Accessed: 8 Jan. 2024).

Lundh, F. and Clark, J. (2023). *Image Module — Pillow (PIL Fork) 6.2.1 documentation*. Readthedocs.io. Available at: https://pillow.readthedocs.io/en/stable/reference/Image.html (Accessed: 11 Jan. 2024).

Microsoft (2023). *Security and Privacy in Microsoft Forms*. support.microsoft.com. Available at: https://support.microsoft.com/en-us/office/security-and-privacy-in-microsoft-forms-7e57f9ba-4aeb-4b1b-9e21-b75318532cd9 (Accessed: 15 Dec. 2023).

Norfolk Archives (2022). *Key developments in voting rights - Archives*. Norfolk.gov.uk. Available at: https://www.archives.norfolk.gov.uk/help-with-your-research/family-history/electoral-registers/key-developments-in-voting-rights (Accessed: 13 Jan. 2024).

Osho, O., Yisa, V.L. and Jebutu, O.J. (2015). *E-voting in Nigeria: A survey of voters' perception of security and other trust factors*. IEEE Xplore. doi:https://doi.org/10.1109/CYBER-Abuja.2015.7360511.

Park, S., Specter, M., Narula, N. and Rivest, R.L. (2021). Going from bad to worse: from Internet voting to blockchain voting. *Journal of Cybersecurity*, 7(1). doi:https://doi.org/10.1093/cybsec/tyaa025.

PythonAnywhere (2022). *About us: PythonAnywhere*. www.pythonanywhere.com. Available at: https://www.pythonanywhere.com/about/company_details/ (Accessed: 8 Jan. 2024).

Ranjan, D. (2023). *Exploring the Pros and Cons of Flask for Web Development in 2023*. www.linkedin.com. Available at: https://www.linkedin.com/pulse/exploring-pros-cons-flask-web-development-2023-deepak-ranjan-4ypnf (Accessed: 15 Jan. 2024).

Ronacher, A. (2023). *Welcome to Flask — Flask Documentation (3.0.x)*. flask.palletsprojects.com. Available at: https://flask.palletsprojects.com/en/3.0.x/.

Scytl (2021). *Which Countries Use Online Voting?* EDGE Elections. Available at: https://medium.com/edge-elections/which-countries-use-online-voting-3f7300ce2f0.

Shanthinii, S.P., Usha, M. and Prittopaul, P. (2023). A Survey Based on Online Voting System Using Blockchain Technology. pp.209–216. doi:https://doi.org/10.1007/978-981-19-7169-3_19.

Smys, S., Balas, V.E. and Palanisamy, R. (2022). *Inventive Computation and Information Technologies: Voter ID Card and Fingerprint-Based E-voting System*. Springer, pp.89–105.

SQLite (2023). *About SQLite*. Sqlite.org. Available at: https://www.sqlite.org/about.html (Accessed: 11 Jan. 2024).

Stratis, K. (2023). *Face Recognition with Python, in Under 25 Lines of Code – Real Python*. realpython.com. Available at: https://realpython.com/face-recognition-with-python/ (Accessed: 3 Dec. 2023).

Summit (2023). *What are the Advantages of SQLite Database for*. perfectelearning.com. Available at: https://perfectelearning.com/blog/what-are-the-advantages-of-sqlite-database-for (Accessed: 15 Jan. 2024).

Tillman, M. (2021). *What is Apple Face ID and how does it work?* Pocket-lint. Available at: https://www.pocket-lint.com/phones/news/apple/142207-what-is-apple-face-id-and-how-does-it-work/ (Accessed: 15 Jan. 2024).

Toynbee, P. (2022). Call these voter ID laws what they really are: voter suppression and an attack on young people. *The Guardian*. 25 Nov. Available at: https://www.theguardian.com/commentisfree/2022/nov/25/voter-id-laws-what-they-really-are-voter-suppression-and-an-attack-on-young-people (Accessed: 4 Jan. 2024).

Uberoi, E. and Johnston, N. (2023). Voter ID. *commonslibrary.parliament.uk*. Available at: https://commonslibrary.parliament.uk/research-briefings/cbp-9187/ (Accessed: 23 Jul. 2023).

UK Parliment (2019). *19th century elections*. UK Parliament. Available at: https://www.parliament.uk/about/living-heritage/transformingsociety/electionsvoting/elections-and-voting-in-the-19th-century/reforming-election-methods/controverted-elections/ (Accessed: 12 Jan. 2024).

Yadav, P. (2023). *OCR: Extract Text from Image In 8 Easy Steps*. Medium. Available at: https://medium.com/@pawan329/ocr-extract-text-from-image-in-8-easy-steps-3113a1141c34 (Accessed: 1 Dec. 2023).

Zeng, G., He, M., Yiu, S.M. and Huang, Z. (2021). A Self-Tallying Electronic Voting Based on Blockchain. *The Computer Journal*. doi:https://doi.org/10.1093/comjnl/bxab123.

APPENDICES

Appendix A. APPROVED DISSERTATION PROPOSAL

Computing

CSCK700 - Computer Science Capstone Project

Project Proposal

Student's Name	Cheylea Hopkinson
Student's Number	
Student's Email Address	C.Z.L.Hopkinson@liverpool.ac.uk
The MSc Programme	Master of Computer Science
Project Title	Exploring Solutions to Internet Voting in Government Elections in the UK
Version Number of the Proposal	v.1.3
Final Dissertation Submission Date	15/01/2024
Proposal Submission Date	05/06/2023
Name of Dissertation Advisor (DA)	Andrea Corradini
Class Start Date	11/04/2023
Name of Dissertation Lead (DL):	Kathleen Kelm
Ethics Approval Needed?	Yes

Proposal Approval *[Do not fill out this section. To be completed by the Dissertation Lead & Dissertation Advisor]*	
Proposal approved by	*To be filled in by the DA*
Date of the approval (DA)	*To be filled in by the DA*
Date of approval confirmed by the Dissertation Lead	*To be completed by the Dissertation Lead*

SPONSOR (if any)

Sponsor's Details: N/A

Sponsor's Background: N/A

Sponsor's Agreement: N/A

PROJECT

The Project Aims and Objectives:

The main objective of this project is to propose an IT system for electronic voting (e-voting) that addresses some of the existing concerns with using e-voting systems within UK government elections. There are two types of e-voting, in-person voting machines and votes cast remotely using the internet (Faruk et al., 2022). For this project, we will focus on internet e-voting. Despite applied technologies such as blockchain that can record immutable votes (Faruk et al., 2022) and e-voting systems existing in other countries – many issues still preside within the topic which prevents rollout in the UK. This includes threats to security, transparency of the vote, and the possibility of election fraud (Mackenzie, 2019). However, finding a robust solution to internet e-voting could have many advantages, such as cost savings, accessibility, and speculations that it could improve voter turnout for young people (Mackenzie, 2019).

This project will produce an internet e-voting system that satisfies the following:

- Incorporate a remote identification check system to minimise system abuse and prevent multiple votes from a single voter.
- Allow voters to self-verify that their cast vote is identical to the vote received.
- Maintain anonymity for the voter throughout the above aims.
- Uphold two-way transparency between voter and governing body.

These aims will be addressed by producing an internet e-voting application that incorporates a solution to satisfy the aims and then evaluated to verify its effectiveness.

In the table below, please state your dissertation question(s); the research methods you will use to guide the development of your IT artefact; the kind of IT artefact you will produce; and how you will evaluate the IT artefact in the light of the dissertation question(s)

Step	Short Description
Dissertation Question(s)	• Can an internet e-voting system identification check be remote whilst ensuring accuracy and voter anonymity? • Would an internet e-voting system compromise the security of the vote casting? • Can an internet e-voting system provide two-way transparency between voter and governing body?
Research Methods	This project will involve several research methods, taking an overall mixed-method approach. **Qualitative analysis of existing solutions and case studies:** • Literature review to understand the current UK attitude towards e-voting, as well as the existing disadvantages of paper votes. • Case studies to examine examples of existing e-voting systems and their advantages, disadvantages, and lessons learned. **Mixed-method analysis of IT solution:** The artefact will undergo three types of testing to analyse its effectiveness: • Experiment approach by running a voting simulation, then determining if the solution effectively meets resolution criteria for both identification and voter self-audit. • Then the artefact will be subjected to multiple attempts to bypass the system, simulating a controlled hack attempt. • Finally, user testing and survey method to assess the suitability of implementation and if it is transparent and trustworthy to the user.
IT Artefact	A secure e-voting application that can be accessed and used via the internet. Will contain an online identification process, as well as a process for the voter to self-audit their cast vote.
Evaluation	The artefact will be assessed on its ability to meet the aims of the project by simulating a voting process and analysing its effectiveness. This will include testing the effects of malicious interference on it and the artefact's trustworthiness thereafter. The artefact will be reviewed by a voluntary sample of the UK population, and a user survey will be conducted afterwards to gauge their perception of the system and their thoughts on its transparency and trust. Results will be analysed and discussed alongside the potential benefits and risks of its implementation, including the ethical, legal, and social issues (ELSI).

Project Outline

The project will follow these main steps, using a mixed-method methodology, combining qualitative and quantitative efforts research.

- Examination of existing voting solutions, the existing issues as they stand in the UK for why electronic voting has not been implemented, including difficulties in being transparent to the

public with emerging technologies such as blockchain and establishing trust in electronic systems.
- Reviewing an internet e-voting framework and examining the security issues between user voting and information storage.
- Create an IT artefact that uses blockchain, an online identification process and an expiring secret word system for self-vote verification to contribute to the body of solutions for internet e-voting.
- Run simulations on the IT artefact and analyse its effectiveness and risk from the perspective of the governing body.
- Allow users to review the system and survey for an initial opinion on internet e-voting and levels of confidence in the IT artefact.
- Critically analyse the results and answer the dissertation questions.

The findings from the above will be collated to summarise the current mindset around internet voting. The project will examine the potential ethical, legal, and social issues (ELSI) and risks alongside the results and will discuss whether the IT artefact could be a viable solution that satisfies the aims.

Literature Survey / Resources' List:

A Survey Based on Online Voting System Using Blockchain Technology (Shanthinii, M. Usha and P. Prittopaul, 2023): Establishes the possibilities with blockchain using a comparative study and notes in future work the need for added security to the solution.

Electronic Voting System Using an Enterprise Blockchain (Denis González et al., 2022): Details how a blockchain system can work for electronic voting using two organisations and voter signature encryption.

BieVote: A Biometric Identification Enabled Blockchain-Based Secure and Transparent Voting Framework (Faruk et al., 2022): An example of a blockchain-based secure system combined with identification technology.

End-to-End Verifiable E-Voting Trial for Polling Station Voting (Hao et al., 2020): Example of trialling a receipt printing system in the UK and demonstrates a system for confirming votes to prevent mistakes in casting. Also contains survey information indicating the reluctance/enthusiasm for electronic voting.

A Self-Tallying Electronic Voting Based on Blockchain (Zeng et al., 2021): Example of blockchain application to e-voting.

Scholarly Contributions of the Project

In the UK, we still use a paper system for voting. Electronic voting in government is a highly contested political subject across the world with caution exercised in the UK due to the concerns outlined in the aims and objectives. This is similar for other countries, such as France, who concluded against electronic voting in 2017 (Reuters, 2017).

The overall scope of the field has many areas with problems that require solving, and this project will focus on the first step of an end-to-end verifiable system: cast as intended (Hao et al., 2020). This includes the fundamental factor verifiability that a vote has been unchanged (Denis González et al., 2022) and, for the specific caster, that vote is the intended vote. Although something like blockchain as a data storage system has ways to verify voting while maintaining anonymity, the solution alone may be too confusing or complex for a regular member of the public to trust (Abuidris, Kumar and Wenyong, 2019).

This project takes a new approach to the topic by allowing voters to self-verify their vote for a short period after the vote has been committed. This is done by submitting a secret word unique to the user and their polling area, which is encrypted alongside their voting choice. Once committed, there will be a small window of time where the voter can view their vote using their secret word to confirm the vote is what they cast and verify that between casting the vote and storing the information in a database it has not been compromised. The application also includes ID checking for voting eligibility, which is now a standard requirement in the UK since 4th May 2023 (The Electoral Commission, 2023).

Overall, e-voting is a dividing topic across different nations and requires continual research and innovation to allow confident decision-making in its implementation/rollout for the government and its public. This project aims to add to this knowledge by testing this new method and its perception by the public.

Description of the Deliverables:

IT Artefact: The product will be a website application to collect internet e-votes via a user interface (UI). The UI will be connected to two blockchain databases, one for 'voter identification' and one for 'vote casting', using encryption for security.

The artefact will be designed with the following features:

- Identification system to identify the candidate, such as facial recognition or other remote photo ID checking methods, and reject if the IDs do not match, they have already voted or are ineligible to vote.
- Basic information on how the voting system works.
- Basic information on candidates and how to vote.
- User interface to select the votes and commit the final vote alongside secret word. Secret words are unique to the user and their polling area. If someone else has used the word already, this wouldn't be accepted. Identifiable words, such as names and addresses, will also be rejected.
- System for the voter to access their vote for a limited time using their secret word.

Simulation Results: A voting scenario will be simulated alongside a simulated 'attack' to demonstrate the effectiveness of the technological solution for identification and for auditing vote accuracy.

User Survey Results: Users will review the artefact and complete a survey around various aspects of the project that also captures their current position on internet e-voting. The sample will aim to be diverse in age range, using the UK population age proportion as a guide (Gov.uk, 2018) and scaled to not include under 18s in the sample: 18 – 25 10.5%, 25 – 39 25.5%, 40 – 59 26.3% and 60+ 30.8%. Results will be provided as a question-answer analysis across different notable groups. Results will be summarised within the dissertation paper.

Evaluation Criteria:

To be successful, the following criteria must be met:

- In all cases, voter identification can be verified whilst maintaining anonymity.

- Voters can self-verify their votes without compromising the security of the vote 100% of the time.
- The system is clearly understandable by most users based on the survey results.
- Any attack on the system can be identified or prevented.

The analysis of simulations of the IT artefact will provide insight into how effectively the solution works as verification and assess its level of vulnerability. This will be accompanied by a critical analysis of the potential disadvantages of implementing such a system. This will include an overview of ELSI impacts that may address questions about its risks. Survey results will then produce an understanding of if this solution, or at least elements of it, is something that could be used and accepted by the public if rolled out. The combined findings will answer the dissertation questions.

Resource Plan:

Resource	How to source	Cost
Participants for the testing and survey	Sourced using free online and local advertising methods (limited to UK participants).	Free
IT artefact software	Produced using Python for the backend development to create a blockchain database, with encryption steps for voter eligibility and casting. I will consider using open-source technology for ID-checking software, such as Deepface (Traichuk, 2021). The user interface will use HTML and CSS.	Free
Survey Platform	Use a free survey platform such as Microsoft Forms or Google Forms	Free

Project Plan and Timing

The below details the plan for this project, including the formal assessment deadlines.

Milestone	Date
Proposal	8th June 2023
Ethical Approval Form	26th June 2023
Specification and Design Report	31st July 2023
Week by week development plan produced	31st July 2023
Test version of IT Artefact ready	***2nd October 2023***
Fieldwork for survey begins	***9th October 2023***
Run simulations on artefact	***16th October 2023***
Poster	23rd October 2023
Simulation analysis completed	***27th November 2023***
Fieldwork for survey ends	***27th November 2023***
Survey analysis completed	***4th December 2023***

Drafts	18th December 2023
IT Artefact	15th January 2024
Video Demonstration (IT Artefact)	15th January 2024
Dissertation	15th January 2024

Risk Assessment:

Potential software-related issues (IT Artefact):

- **Failed Integration:** Most of the artefact will be developed using Python, which will reduce the likelihood of different parts of the project being incompatible.
- **Inoperative:** The artefact design collates well-known existing technologies: remote identification, blockchain and encryption. Therefore, the software will be operational at a prototype level, and any vulnerabilities in the functionality will be highlighted by the simulation testing, which forms part of the answer to the questions the dissertation is asking.

Potential hardware-related issues (IT Artefact):

- **Incompatibility:** to avoid this, the most recently updated software versions possible will be used; with the artefact user interface being designed in such a way to be usable on various screen sizes and standard browsers.

Lack of Participation (User Survey)

To work towards mitigating this risk, the following will be implemented:

- Clear and easy-to-use survey interface that is accessible for different people, with questions that are easy to understand and documentation that details the purpose of the project and how the data will be used.
- A clear plan for the people needed to target for participation from the beginning will help mitigate the possibility of a poor sample.
- Utilising personal network to advertise the survey and highlight the scholarly importance to potential participants to push for more engagement.

If low survey participation is experienced:

- Approach groups containing known required target groups for further attempts at acquiring engagement.

Data Quality (User Survey)

The answers to the survey need to reflect accurately the thoughts of the users of the artefact to be useful. In addition to documentation and clear questioning, a screening question will be present in the survey that could only be answered if the artefact review has been completed. Users that do not pass the screening question will have any survey responses removed to ensure the legitimacy of the survey.

Quality Assurance:

The project plan deadlines will monitor the progress of the project, including the assessment sections of the capstone module. Once the full specification and design plan has been completed, a full week-by-week development plan will be established to keep the rest of the project on track, using 3rd party online tool Trello to monitor individual tasks for completion within the project. This will highlight quickly if the project is falling behind, and actions can be taken to bring it back on course, including contingency plans detailed in the risk assessment section.

The IT artefact will have a suite of unit tests whilst being developed to ensure all functionality remains intact, as well as integration tests for the different parts of the software. Some performance testing will also be conducted to ensure the software runs efficiently.

During the development, consultations with Dissertation Advisor (Andrea Corradini) will occur to advise on progress and advise on areas of concern. Where appropriate, Dissertation Lead (Kathleen Kelm) will also be contacted for feedback.

References

Abuidris, Y., Kumar, R. and Wenyong, W. (2019). A Survey of Blockchain Based on E-voting Systems. *Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications*. doi:https://doi.org/10.1145/3376044.3376060.

Denis González, C., Frias Mena, D., Massó Muñoz, A., Rojas, O. and Sosa-Gómez, G. (2022). Electronic Voting System Using an Enterprise Blockchain. *Applied Sciences*, 12(2), p.531. doi:https://doi.org/10.3390/app12020531.

Faruk, J.H., Islam, M., Alam, F., Shahriar, H. and Rahman, A. (2022). BieVote: A Biometric Identification Enabled Blockchain-Based Secure and Transparent Voting Framework . *Fourth International Conference on Blockchain Computing and Applications (BCCA)*.

Gov.uk (2018). *Age groups*. Service.gov.uk. Available at: https://www.ethnicity-facts-figures.service.gov.uk/uk-population-by-ethnicity/demographics/age-groups/latest (Accessed: 5 May 2023).

Hao, F., Wang, S., Bag, S., Procter, R., Shahandashti, S.F., Mehrnezhad, M., Toreini, E., Metere, R. and Liu, L. (2020). End-to-End Verifiable E-Voting Trial for Polling Station Voting. *IEEE Security & Privacy*. doi:https://doi.org/10.1109/msec.2020.3002728.

Mackenzie, N. (2019). *Why can't British people vote electronically? Cost, fraud and security all have parts to play*. Metro. Available at: https://metro.co.uk/2019/12/11/general-election-voting-online-would-be-a-mess-and-prone-to-hacking-11584494/ (Accessed: 23 Apr. 2023).

Reuters (2017). France drops electronic voting for citizens abroad over cybersecurity fears. *Reuters*. 6 Mar. Available at: https://www.reuters.com/article/us-france-election-cyber-idUSKBN16D233 (Accessed: 25 May 2023).

Shanthinii, S.P., M. Usha and P. Prittopaul (2023). A Survey Based on Online Voting System Using Blockchain Technology. pp.209–216. doi:https://doi.org/10.1007/978-981-19-7169-3_19.

The Electoral Commission (2023). *Voting at the polling station with photo ID on 4 May*. www.electoralcommission.org.uk. Available at: https://www.electoralcommission.org.uk/voting-polling-station-photo-id-4-may (Accessed: 27 May 2023).

Traichuk, A. (2021). *6 Best Open-Source Projects for Real-Time Face Recognition | HackerNoon.* hackernoon.com. Available at: https://hackernoon.com/6-best-open-source-projects-for-real-time-face-recognition-vr1w34x5 (Accessed: 27 May 2023).

Zeng, G., He, M., Yiu, S.M. and Huang, Z. (2021). A Self-Tallying Electronic Voting Based on Blockchain. *The Computer Journal*. doi:https://doi.org/10.1093/comjnl/bxab123.

Appendix B. SPECIFICATION & DESIGN REPORT

Student's Name: Cheylea Hopkinson

Student's Number:

Student's Email Address: C.Z.L.Hopkinson@liverpool.ac.uk

Project Title: Exploring Solutions to Internet Voting in Government Elections in the UK

Name of Dissertation Advisor (DA): Andrea Corradini

Name of Dissertation Instructor (DI): Kathleen Kelm

A. The Specification

Project Context, Aims, Objectives, Ethical Considerations and Outcomes

The Context of the Research

The local government elections that took place on 4th May 2023 were the first time in which voters were required to show photo identification to vote in person (Uberoi and Johnston, 2023). This change brought about mixed responses from the UK public and was not without controversy (Moorhouse, 2023), with poll clerks reportedly receiving abuse on the day (Sefton Council, 2023). This effectively highlights how changes to a voting system have the potential to cause discontent amongst the public.

Electronic voting (e-voting) systems exist both in theory and practice throughout the world, such as Estonia which uses remote e-voting for its national and local elections (Scytl, 2021). However, e-voting is not without risks or drawbacks. In the UK, part of the reason why e-voting has not been adopted is due to concerns about election fraud, security threats, and transparency (Mackenzie, 2019). However, undeniably, there are potential advantages, such as accessibility and saving costs (Mackenzie, 2019). This research intends to add to the discussion of the viability, credibility, and practicality of e-voting systems, using an original e-voting concept. Future solutions will likely need to draw on this body of evidence, to ensure e-voting is trusted and robust enough to be publicly accepted.

The Problem Statement

The goal of e-voting is to find a technological solution where its benefits outweigh the risks and can be trusted by both voters and governing body. This project will focus on internet e-voting, rather than electronic voting machines. Some proposed solutions include progressive elements, such as harnessing blockchain technology (Faruk et al., 2022), but there is not yet one solution that solves all.

One existing problem is how to verify voting is cast and counted accurately. Hao et al. (2020) presents the definition of a fully verifiable system as requiring a voter to verify their vote was cast for the right person, is recorded correctly in the system and a public observer can verify votes are tallied correctly (Hao et al., 2020). However, Denis González et al. (2022) establishes several other criteria: untraceable, precise, accurate, unchangeable, verifiable, receipt-free, dispute-free, accessible, and decentralised.

There are various examples of blockchain systems that successfully solve many of the concerns around a centralised e-voting system; as demonstrated in *'Electronic Voting System Using an Enterprise Blockchain'* (Denis González et al., 2022) and *'A Self-Tallying Electronic Voting Based on Blockchain'* (Zeng et al., 2021). However, these do not provide fully secure solutions that are robust enough to be brought into production, and most papers recommend more research in their conclusions. Other papers, such *as 'BieVote: A Biometric Identification Enabled Blockchain-Based Secure and Transparent Voting Framework'* (Faruk et al., 2022) explore the issues of identifying voters accurately to avoid voter fraud. Ahsan (2019) presents a solution in *'Coercion-Resistant E-Voting Scheme with Blind Signatures'* to avoid people being coerced when voting, but also demonstrates that the system they designed does not fully cover voter verifiability.

Hence, the general problem is to find a solution that can satisfy all criteria. For this project, it will attempt to propose a solution that solves some of these issues, to move research closer to finding a whole.

The Dissertation Question(s)

The following questions will be answered within the dissertation:

1. Can an internet e-voting system identification check be remote whilst ensuring accuracy and voter anonymity?
2. Would an internet e-voting system compromise the security of the vote casting?
3. Can an internet e-voting system provide two-way transparency between voter and governing body?

These questions will be answered by combining testing of an electronic voting system through means of simulations and user review via a survey.

Ethical Implications

A survey will be conducted during the research which will ask users to review the electronic voting tool and basic questions around their demographics and views on electronic voting. Therefore, this will require both an ethical approval application and a Data Protection Impact Assessment (DPIA) since the survey will ask for an opinion on a political topic. The main risk to participants is the exposure of their information if it is not kept confidential, which will be mitigated by collecting minimal identifiable information and anonymising all data within the final dissertation.

The survey will take place remotely and participants will be sourced using online networks and forums. The participants will be restricted to adults over the age of eighteen that have previously voted in a local or general election. This is to limit research to those currently familiar with the UK voting process.

Answers will be used to help evaluate the electronic voting tool. This research will contribute to answering dissertation question three, by determining if the prototype tool, or a version of it, could satisfy two-way transparency.

The Anticipated Outcomes

The outcome of this project is to determine if a particular e-voting model could satisfy the three dissertation questions; and if not, what barriers remain?

As established in the problem statement, further research, with different combinations of methods, is needed to continue to bring progress closer to creating a voting system that truly satisfies all aims.

The project will explore existing solutions and propose a new one developing an IT artefact that satisfies the following goals, as presented in the dissertation proposal (Appendix A).

- Incorporate a remote identification check system to minimise system abuse and prevent multiple votes from a single voter.

- Allow voters to self-verify that their cast vote is identical to the vote received.
- Maintain anonymity for the voter throughout the above aims.
- Uphold two-way transparency between voters and governing body.

The IT artefact attempts to combine several features with an original approach to vote verification by voters. It will be evaluated in its effectiveness as a tool in voting simulations, as well as the tool's acceptance of user opinions, using survey results. This research, and others like it, is a vital step in the evolution of e-voting in the UK and indicates the direction of travel progress will need to take on a backdrop of shifting public opinions.

Literature Survey

Risks and Opportunities of Blockchain Based on E-Voting Systems

Abuidris, Y., Hassan, A., Hadabi, A. and Elfadul, I. (2019). *Risks and Opportunities of Blockchain Based on E-Voting Systems*. IEEE Xplore. doi:https://doi.org/10.1109/ICCWAMTIP47768.2019.9067529.

This paper summarises the different advantages and disadvantages of blockchain and caters to audiences of both users and developers alike. Blockchain is useful for e-voting systems because data stored using it cannot be altered and can more effectively prevent unauthorised alteration. Meaning, if used in a voting system, it would be difficult to change the values of votes once they are cast and committed. However, although blockchain introduces many advantages and solutions to security, he details how not all scenarios are solved and introducing a system into democracy may have adverse results. The paper also identifies disadvantages, including vulnerabilities such as: not being tested on a full scale; limited scope to prevent vote-buying; and the difficult balance required between voter eligibility verification and voter anonymity.

The paper captures the general problems that arise when attempting to implement e-voting with blockchain. It emphasises in the conclusion that this technology is still in its early life and would demand far more research to develop something fully successful. This sets the stage for where the direction of research for e-voting needs to go.

Debate: safeguarding democracy during pandemics. Social distancing, postal, or internet voting—the good, the bad or the ugly?

Krimmer, R., Duenas-Cid, D. and Krivonosova, I. (2020). Debate: safeguarding democracy during pandemics. Social distancing, postal, or internet voting—the good, the bad or the ugly? *Public Money & Management*, pp.1–3. doi:https://doi.org/10.1080/09540962.2020.1766222.

This study was conducted as a result of the effects of the Covid-19 pandemic and raises questions about how to maintain democracy during times when people may be confined to their homes and unable to be within a certain distance of other people because of their health.

It notes how there is a choice between whether to hold an election, and if it is held, how the system needs to be adapted. Each scenario is examined. Adding health protection only, for example, is said to guarantee a turnout decrease and potentially increase infection among the population as it increases the number of potential exposures. Postal votes would eliminate the health risk for most of the population but may put more health strain on postal workers during elections and would assume the postal system is unaffected by the conditions of the pandemic, which is unlikely. The final scenario is internet voting, which would not have delivery-related issues but has its own set of risks that require mitigation – making it not workable to implement in the short term.

To conclude, this paper highlights the impact of elections when in-person paper voting may cause health risks to the population and highlights the need to develop a long-term solution such as internet voting if something like the pandemic were to occur again.

A Survey Based on Online Voting System Using Blockchain Technology

Shanthinii, S.P., Usha, M. and Prittopaul, P. (2023). A Survey Based on Online Voting System Using Blockchain Technology. pp.209–216. doi:https://doi.org/10.1007/978-981-19-7169-3_19.

The context for this article is the dropping rates of voter participation in India, implying that the result of this is a lack of democracy. It argues that the only solution to combat this issue is to create a mobile or web application that citizens of India can use to vote in any location. This, however, is not addressed in the paper itself.

The paper focuses on comparing existing blockchain voting systems, focusing on Ethereum-based blockchain and analyses the current potential and its disadvantages. It concludes that Ethereum is an improvement on other existing frameworks but requires more security, such as biometric id checks using fingerprint scanners. The paper also touches on transparency as an ongoing issue but proposes no solution for this.

Overall, the paper establishes the potential of blockchain within e-voting systems using comparative study but makes clear it is not part of the problem, and further research is required to design a full end-to-end secure system. Despite referring to social issues in the abstract, the paper misses the opportunity to establish if this would truly be a solution to India's voting participation problem and whether Indian citizens would be accepting of an e-voting system.

BieVote: A Biometric Identification Enabled Blockchain-Based Secure and Transparent Voting Framework

Faruk, J.H., Islam, M., Alam, F., Shahriar, H. and Rahman, A. (2022). BieVote: A Biometric Identification Enabled Blockchain-Based Secure and Transparent Voting Framework . *Fourth International Conference on Blockchain Computing and Applications (BCCA)*.

Identification is mentioned in papers such as *'A Survey Based on Online Voting System Using Blockchain Technology'* (Shanthinii, Usha and Prittopaul, 2023) as a form of added security for an e-voting system. The BieVote shows how a blockchain-based e-voting system can be used with biometric identification technology (facial and fingerprint recognition) and asserts that the conceptual model presented will be further researched to create a "real-world application" (Faruk et al., 2022, p.7).

It conducted a literature review focused on Hyperledger Fabric-based blockchain systems with typical blockchain advantages, such as guaranteeing anonymity and being decentralised. This is then used to design the conceptual BieVote architecture that includes the biometric identification process to verify the identity of the voter.

It is a start in examining how blockchain, a technology that prevents tampering with the information once stored, and biometric identification, a potential necessity to avoid voter fraud when voting from home, can create a stronger, more secure system. However, as it is only conceptual at this stage, it is difficult to verify how much a system can satisfy all criteria such as transparency.

End-to-End Verifiable E-Voting Trial for Polling Station Voting

Hao, F., Wang, S., Bag, S., Procter, R., Shahandashti, S.F., Mehrnezhad, M., Toreini, E., Metere, R. and Liu, L. (2020). End-to-End Verifiable E-Voting Trial for Polling Station Voting. *IEEE Security & Privacy*. doi:https://doi.org/10.1109/msec.2020.3002728.

This study discusses a first-of-its-kind e-voting trial in the UK that occurred in 2019. It uses an example of an in-person e-voting system and uses receipt printing as part of the voting process. It focuses on ensuring that voters feel confident the correct vote they have selected has been cast and contains a system that both confirms the cast votes and prevents mistakes in casting. Voters might walk out with up to one confirmed voting receipt and any number of cancelled voting receipts, depending on how they tried to vote. It was found that the usability of the system had an excellent score.

Each voter was surveyed after they voted using the system, with 93 returned surveys. More than half the participants stated they preferred the e-voting system as the method felt "easy" and "safe" (Hao et al., 2020, p8). However, there were still participants that felt the security of e-voting was still an issue and maintained their preference for paper ballots. There are limitations to these results, such as the size of the survey and was limited to those local to where the study was conducted. What is missing from this paper is whether it was easy for voters to verify their vote and understand how it works.

Electronic Voting System Using an Enterprise Blockchain

Denis González, C., Frias Mena, D., Massó Muñoz, A., Rojas, O. and Sosa-Gómez, G. (2022). Electronic Voting System Using an Enterprise Blockchain. *Applied Sciences*, 12(2), p.531. doi:https://doi.org/10.3390/app12020531.

This paper outlines potential flaws of existing electronic solutions that use a centralised approach, as opposed to blockchain, including how data can be manipulated, either intentionally or by accident. It notes existing problems with permissionless blockchain as a solution, such as high-power consumption and how the model presented in the article can tackle all these issues. It discusses using Enterprise blockchain to create a secure system that preserves the privacy of voters, is more efficient, and can decrease vote counting time.

There are several criteria the paper presents in the introduction to what is required of an e-voting system, which is established in the Problem Statement section of this document. These themes arise in many e-voting papers, but what is notable is the receipt-free criteria - that a vote should not create a receipt as it may be problematic to produce something that could show how a voter voted. Hao et al. (2020) demonstrates that this does not necessarily mean physical receipts are not a possibility in a voting system, but only that the receipt itself cannot be used to prove how you voted. What's not addressed is the issue of transparency, and how easily the system presented in the paper could be understood by a voter.

A Self-Tallying Electronic Voting Based on Blockchain

Zeng, G., He, M., Yiu, S.M. and Huang, Z. (2021). A Self-Tallying Electronic Voting Based on Blockchain. *The Computer Journal*. doi:https://doi.org/10.1093/comjnl/bxab123.

Zeng et al. (2021) present the problem of blockchain-based systems requiring a central representative to count votes or a limit to how the number of votes that can be counted. It is established that despite this blockchain has advantages, such as costing $0.7 per voter when using an Ethereum blockchain system, compared to $2.77 using paper. In response, the paper presents a solution to this problem by creating a self-tallying system.

The system proposed is compared to other schemes and shows that it is more secure and can be counted with no need to trust an independent third party to complete the tallying. However, a new problem arises as a result, in which whoever the last person to vote is will know the total result ahead of time and may amend their vote based on this information. This is classified as "last voter

privilege" (Zeng et al., 2021, p3030). The paper discusses potential workarounds but concludes this is an issue not yet solved.

Overall, there is clear merit to the system based on its advantage compared to others within the paper but is still not a perfect solution – requiring further research and development to find a full resolution.

E-voting in Nigeria: A survey of voters' perception of security and other trust factors

Osho, O., Yisa, V.L. and Jebutu, O.J. (2015). *E-voting in Nigeria: A survey of voters' perception of security and other trust factors*. IEEE Xplore. doi:https://doi.org/10.1109/CYBER-Abuja.2015.7360511.

Osho, Yisa, and Jebutu (2015) performed this survey in 2015 after partial e-voting was implemented in Nigeria for the first time. The paper details how the existing method of conducting elections was losing trust and therefore required new ideas and approaches to regain vote integrity.

The survey found that many of the participants would prefer to vote by electronic means, except for those that reported low IT proficiency. It claims that significant effort would be required to increase trust among this demographic of voters and any e-voting system must maximise its ease of use. To enhance this trust, they describe how e-voting systems must have five factors: "privacy, reliability, ease of use, security, and availability" (Osho, Yisa and Jebutu, 2015, p.207). There is also the need to increase the proportion of Nigerians that have access to the Internet for e-voting to be successful (Chikioke-Keme, 2019).

One drawback to the survey is the minimal diversity in the participants, as most were young males with just over half describing themselves as IT proficient. This survey is also nearly ten years old, and advancements in technology may impact how participants would now view security and trust.

Formalization of Receipt-Freeness in the Context of Electronic Voting

Bräunlich, K. and Grimm, R. (2011). Formalization of Receipt-Freeness in the Context of Electronic Voting. *2011 Sixth International Conference on Availability, Reliability and Security*. doi:https://doi.org/10.1109/ares.2011.25.

Receipt-freeness is the idea that after voting, a voter cannot possess any kind of receipt that can reveal how a voter cast their vote. This is important in maintaining secrecy and protecting voters. This paper focuses on presenting a security model that specifically targets receipt-freeness. It also refers to the "Common Criteria for Information Technology Security Evaluation (CC)" (Bräunlich and Grimm, 2011, p.119) that uses a scale to evaluate the level of assurance of security for a system. It notes that for elections a higher evaluation level is required to be reached compared to non-election e-voting systems.

Within the paper, it presents a security theorem that states if a voting system is secure, in terms of receipt-freeness, and data in transmission satisfies a set of four rules, then the subsequent state of the voting system is also secure. The rules, constraints, and definitions are drawn from various other academic sources. It concludes the model presented could satisfy a high CC evaluation.

Finally, the paper recommends the next step in the research is to formalise verifiability for both the individual voter and the general population to highlight any areas of conflict between this voting requirement and receipt-freeness.

Coercion-Resistant E-Voting Scheme with Blind Signatures

Ahsan, A. (2019). Coercion-Resistant E-Voting Scheme with Blind Signatures. *2019 Cybersecurity and Cyberforensics Conference (CCC)*. doi:https://doi.org/10.1109/ccc.2019.00009.

Ahsan (2019) proposes a different e-voting scheme, utilising blind signatures, which can be a solution to some of the security requirements for e-voting. The paper defines coercion-resistance as having receipt-freeness and that someone who is potentially coercing a voter cannot force a voter to not vote or vote in a specific way.

The system works by allowing a voter to create a genuine login and many fake logins with various passwords. Any votes committed with the fake logins will be ignored and only ones cast with a genuine login would be accepted. Steps are taken to ensure this cannot be detectable in all realms and fake passwords cannot be requested in excessive bulk.

The paper achieves proposing a system that would avoid coercion, however, there still exists vote verifiability at an individual level, which is not covered by this model. It states that coercion-resistance conflicts directly with the verifiability property "tallied-as-recorded" (Ahsan, 2019, p149) where voters would require the ability to check if the vote cast is counted in the results. This means this model couldn't work as-is for an end-to-end verifiable system (Ahsan, 2019, p149).

Conduct of the Project

Through the literature survey and research conducted so far, blockchain has shown considerable potential within e-voting systems, both in practice and theory. While there are still issues remaining around its user understanding and overall public trust in a complex, technological system, when combined with other methods, it can become more than the sum of its parts.

Therefore, this project will incorporate blockchain technology into an e-voting tool, at the centre of the design, and will include a self-verification element to help foster trust within the potential voter. The research will also examine various identification methods, such as biometric identification, that could be used in the project – one of which will be selected.

Python has been chosen as the language, as it can develop blockchain databases and has available open-source technology for identification checking. HTML and CSS will be used for the user interface as the design will be simple to not overcomplicate the user experience. All three languages have been extensively used by the researcher, although building blockchain databases and identification will be a new endeavour and requires some skill development.

Exploring the effectiveness of the artefact will be done using a mixed-method research approach, as referenced in the dissertation proposal (Appendix A) and the Design section of this document. The core approaches to evaluation are the quantitative analysis of simulations and the mixed-method analysis of survey data. Data for simulations will be produced during the tests and the survey will involve approaching potential participants online and using online networks to sample a variety of people.

B. The Design

The created IT artefact will be an e-voting tool with the following features:

- Remote access through the internet
- Immutable vote casting
- Prevents multiple voting by the same person
- Remote identification to prevent fraud
- Self-verification system for votes cast
- Instructions on how to vote and information about the candidates

The main IT artefact will comprise all these features, with a separate testing version of the artefact used for user testing, to avoid collecting sensitive identification data. It will be produced using Python, HTML and CSS. It will be assessed using a mixed-method approach.

- A quantitative analysis by running simulations to answer dissertation questions one and two. This will involve simulating the casting of a vote and its security testing.
- A quantitative and qualitative analysis of survey answers submitted by people that have tested the tool.

The dissertation questions aim to test if identification can be effective, if security can be uncompromised, and if two-way transparency can be upheld. The development and evaluation of an e-voting tool with this design will provide answers to these questions. The analysis will help determine if the IT artefact is viable and will contribute to the knowledge and discussion about what is possible, conceivable, and acceptable to the UK public.

There will be two separate databases for voters and votes so that votes cannot be linked to the original voter. The identification process is entirely separate from the voting process. The self-verification system works by asking the voter for a secret word, and there is a short amount of time when the voter can check their vote is cast correctly. The design of the tool will take the following structure, as in Figure 1.

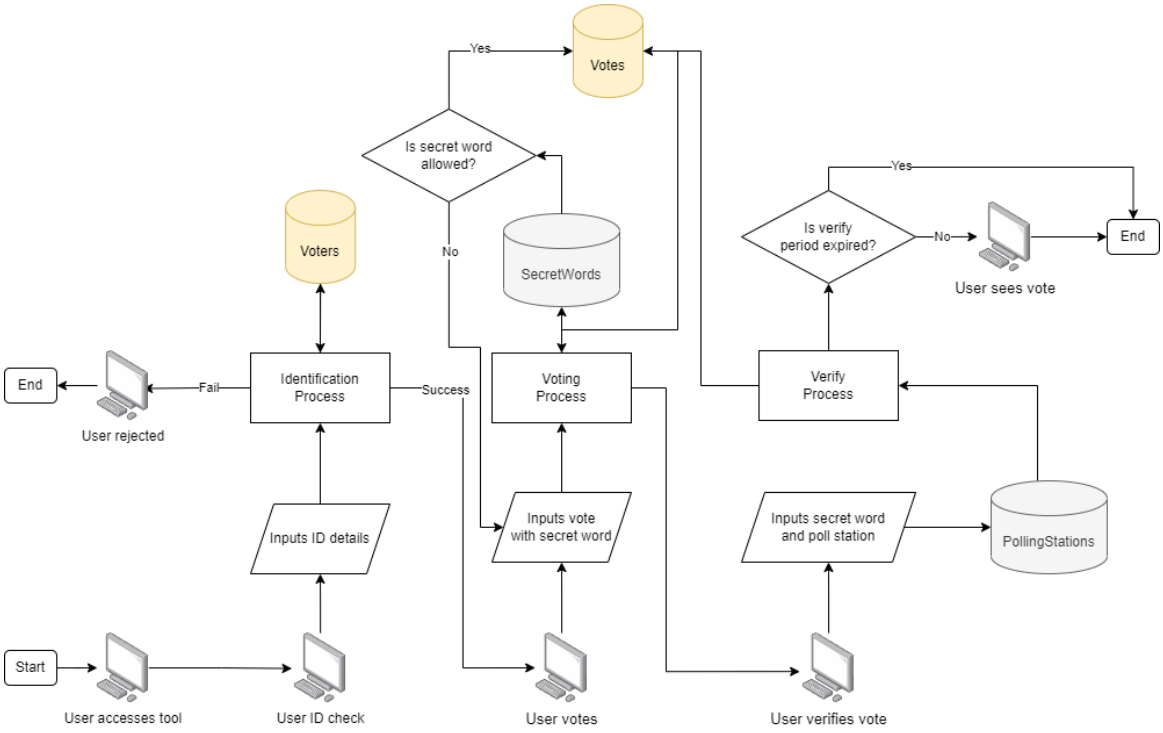

Figure 35 - Flow chart demonstrating the back-end structure of the IT artefact

In the system, data is stored in two blockchain and two read-only databases. One blockchain database is used to record the identity of the voters during the identification process. The other is to record the cast vote themselves. A third database of secret words is present to prevent users from using words that are not allowed, such as identifiable information or inappropriate words. Finally, the last database is to look up the poll station number based on the address provided to get the voting reference. The following pseudocode describes how the system will work, including the interaction of the databases:

```
Check voter eligibility:
Receive input:
   [voter poll number or full name and address]
         Call database ‘voters’ - GET and store as variables (poll-
         number, pollingstationprefix, fullname, address, votingeligi-
         bility, hasvoted)
         If voter not in database:
               Voter eligible fail - User not found
               End
         If votingeligibility is not eligible:
               Voter eligible fail - User not eligible
               End
         If voter hasvoted is yes:
               Voter eligible fail - User already voted
               End
         Else:
               Voter eligible success
   Check voter identification:
   Receive input:
         [identification information]
         If id information matches user:
               Voter identified success
         Else:
               Voter identified fail
               End
   Check secret word:
   Receive input:
         [secret word]
         Call database ‘secretwords’ - GET (secretwords)
         If secret word in database:
               Reject word and show error message on screen
         Else:
               Continue
   Voter votes:
   Receive input:
         [details of vote and secret word]
         Concatenate pollingstationprefix and secret word (votingrefer-
         ence)
         Encrypt details of vote and votingreference
         Call database ‘votes’ - POST (votingreference, details of
         vote, timestamp)
         If POST successful:
               Update hasvoted to yes
               Call database ‘voters’ - PUT (pollnumber, hasvoted)
               If PUT Successful:
               Else:
                     Retry
         Else:
               Retry
   Voter verifies vote:
   Receive input:
         [secret word and (polling station or address)]
         If received address:
```

```
      Call database 'pollingstations' - GET pollingstationpre-
      fix
Concatenate pollingstationprefix and secretword (votingrefer-
ence)
Encrypt votingreference
Call database 'votes' - GET votingreference, timestamp,
votedetails
If timestamp + allowed_time > Now:
      Verification fail - outside of time window
Else:
      Decrypt vote details and display on screen
      Expire window after 30 seconds
```

The design for the user interface is intended to be simple and accessible, guiding the user on how to use the tool. Figure 2 shows an example of how the voting screen may look.

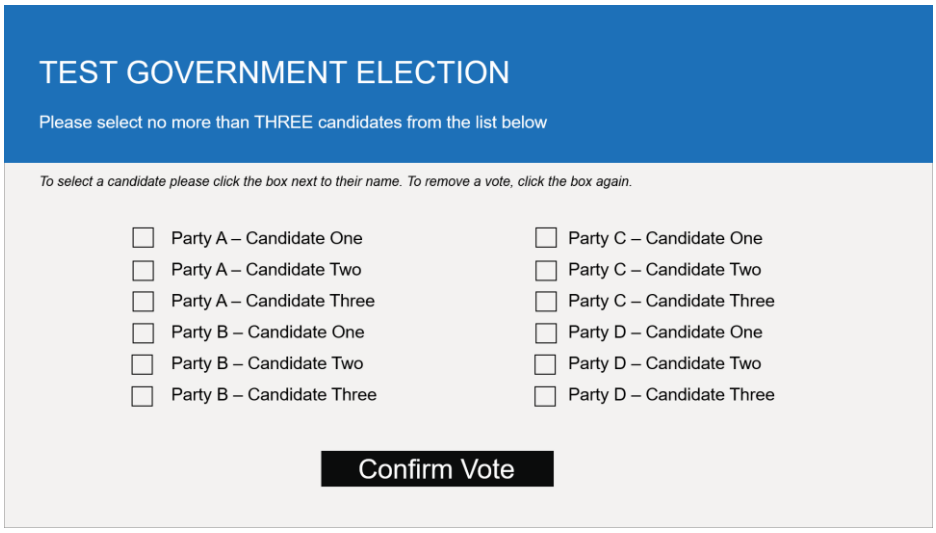

Figure 36 - Example wireframe of user interface of voting page for IT artefact

Evaluation

The evaluation will test three main hypotheses based on the dissertation questions.

$H_{0\text{-}1}$ The e-voting system can identify a user is who they claim to be.

$H_{0\text{-}2}$ The e-voting system is entirely secure and cannot be tampered with undetected by either the public or the government.

$H_{0\text{-}3}$ The e-voting system is trusted by voters.

The first two hypotheses will be proven by running the following simulations.

- A simulated election using test identifications. This will test if remote identification has merit in this context. A threshold for accuracy will be established to pass.
- A simulated 'hack' or attempt to alter the data. This will test if tampering is possible, and if so, if it is easy to identify. This will involve attempting to change data when committing to the blockchain.

For the third hypothesis, a survey will be conducted by users that have reviewed the IT artefact, with age group proportions as stated in the dissertation proposal (Appendix A).

Questions asked will include demographic questions, existing opinions on e-voting, whether users already know about blockchain, and questions about the artefact itself. Full details about the survey questions can be seen in Appendix B. The answers will be analysed to determine if the system can be accepted by the public using hypothesis testing.

C. Statement of Deliverables

Using the specification and design, this section details the project's deliverables.

Poster: This is an intermittent deadline in the project detailing the progress of the research at the time of creation.

IT Artefact: Deliverables related to the artefact will comprise:

- **Electronic Voting Tool:** As stated in the original proposal (Appendix A), the artefact will be a website application with an interactable user interface (UI) that allows the user to vote using the internet. It will use Python, HTML and CSS to produce, and the code will be fully documented with information on how to use it.
- **Video Demonstration:** Alongside the artefact will be a video demonstration of how the voting tool functions, alongside examples and a view of how the databases are updated when in use.

Dissertation: The dissertation will be a comprehensive report that will comprise:

- **Literature Review:** An expanded version of the Literature Review will be completed in this document, with a comparison of articles where pertinent and an overall evaluation of the current context for electronic voting and using it in government elections. This section will also highlight the research gaps which has led to the design of the IT artefact.
- **IT Artefact Design:** Full final design of the IT artefact, including diagrams and code overview, to show how the artefact works and is created.
- **Simulation Design and Results:** There will be two simulations run on the artefact, the first being a basic functionality simulation to ensure the voting tool functions how it is designed to. The second will be a simulation of an "attack" on the system to assess its security.
- **User Survey Results:** A user survey will be conducted to collect the opinion of potential voters about the IT artefact and electronic voting. The results will be collated and discussed if the IT artefact could be trusted.
- **IT Artefact Evaluation:** The combined simulations and user survey results will assess the feasibility of the system and determine answers to the dissertation questions.

D. Project Plan

The table in Project Plan and Timing section in Appendix A contains the goals and dates for the project, including mandatory deadline details. At the time of this document, both the proposal (Appendix A) and ethical approval forms have been completed.

The Gant chart gives a visual representation of the project plan and when each task will be conducted.

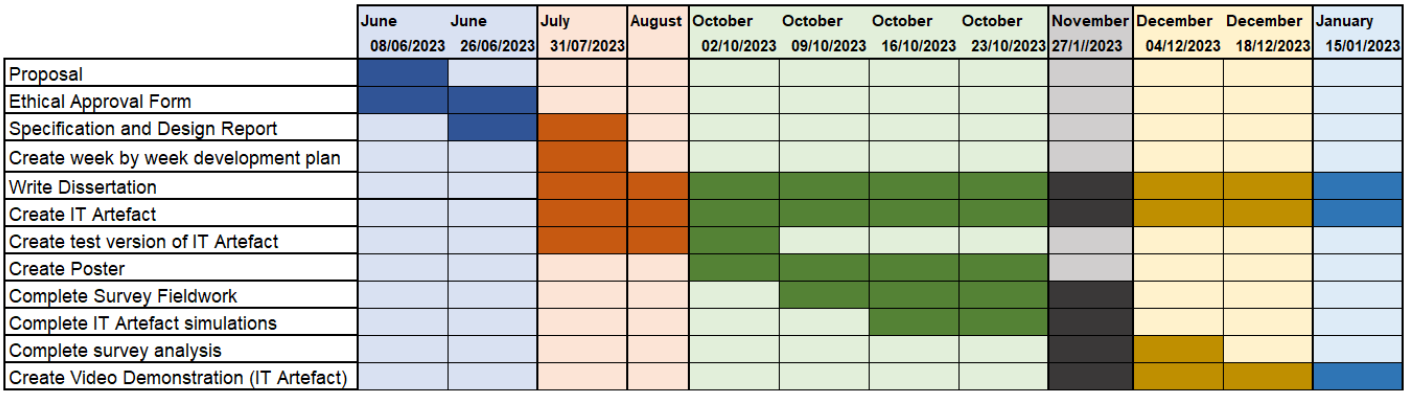

Figure 37 - Gant chart of project plan

References

Abuidris, Y., Hassan, A., Hadabi, A. and Elfadul, I. (2019). *Risks and Opportunities of Blockchain Based on E-Voting Systems*. IEEE Xplore. doi:https://doi.org/10.1109/ICCWAMTIP47768.2019.9067529.

Ahsan, A. (2019). Coercion-Resistant E-Voting Scheme with Blind Signatures. *2019 Cybersecurity and Cyberforensics Conference (CCC)*. doi:https://doi.org/10.1109/ccc.2019.00009.

Bräunlich, K. and Grimm, R. (2011). Formalization of Receipt-Freeness in the Context of Electronic Voting. *2011 Sixth International Conference on Availability, Reliability and Security*. doi:https://doi.org/10.1109/ares.2011.25.

Chikioke-Keme, K. (2019). *Nigeria is not ready for electronic voting*. www.stears.co. Available at: https://www.stears.co/article/nigeria-is-not-ready-for-electronic-voting/ (Accessed: 29 Jul. 2023).

Denis González, C., Frias Mena, D., Massó Muñoz, A., Rojas, O. and Sosa-Gómez, G. (2022). Electronic Voting System Using an Enterprise Blockchain. *Applied Sciences*, 12(2), p.531. doi:https://doi.org/10.3390/app12020531.

Faruk, J.H., Islam, M., Alam, F., Shahriar, H. and Rahman, A. (2022). BieVote: A Biometric Identification Enabled Blockchain-Based Secure and Transparent Voting Framework . *Fourth International Conference on Blockchain Computing and Applications (BCCA)*.

Hao, F., Wang, S., Bag, S., Procter, R., Shahandashti, S.F., Mehrnezhad, M., Toreini, E., Metere, R. and Liu, L. (2020). End-to-End Verifiable E-Voting Trial for Polling Station Voting. *IEEE Security & Privacy*. doi:https://doi.org/10.1109/msec.2020.3002728.

Mackenzie, N. (2019). *Why can't British people vote electronically? Cost, fraud and security all have parts to play*. Metro. Available at: https://metro.co.uk/2019/12/11/general-election-voting-online-would-be-a-mess-and-prone-to-hacking-11584494/ (Accessed: 23 Apr. 2023).

Krimmer, R., Duenas-Cid, D. and Krivonosova, I. (2020). Debate: safeguarding democracy during pandemics. Social distancing, postal, or internet voting—the good, the bad or the ugly? *Public Money & Management*, pp.1–3. doi:https://doi.org/10.1080/09540962.2020.1766222.

Moorhouse, S. (2023). *Leicestershire voters react to new voting ID rules*. LeicestershireLive. Available at: https://www.leicestermercury.co.uk/news/local-news/leicestershire-voters-react-controversial-new-8072852 (Accessed: 23 Jul. 2023).

Osho, O., Yisa, V.L. and Jebutu, O.J. (2015). *E-voting in Nigeria: A survey of voters' perception of security and other trust factors*. IEEE Xplore. doi:https://doi.org/10.1109/CYBER-Abuja.2015.7360511.

Scytl (2021). *Which Countries Use Online Voting?* EDGE Elections. Available at: https://medium.com/edge-elections/which-countries-use-online-voting-3f7300ce2f0.

Sefton Council (2023). *Sefton Council leader 'appalled' at abuse of polling station staff over ID requirements*. www.sefton.gov.uk. Available at: https://www.sefton.gov.uk/mysefton-news/latest-news/sefton-council-leader-appalled-at-abuse-of-polling-station-staff-over-id-requirements/ (Accessed: 23 Jul. 2023).

Shanthinii, S.P., Usha, M. and Prittopaul, P. (2023). A Survey Based on Online Voting System Using Blockchain Technology. pp.209–216. doi:https://doi.org/10.1007/978-981-19-7169-3_19.

Uberoi, E. and Johnston, N. (2023). Voter ID. *commonslibrary.parliament.uk*. Available at: https://commonslibrary.parliament.uk/research-briefings/cbp-9187/ (Accessed: 23 Jul. 2023).

Zeng, G., He, M., Yiu, S.M. and Huang, Z. (2021). A Self-Tallying Electronic Voting Based on Blockchain. *The Computer Journal*. doi:https://doi.org/10.1093/comjnl/bxab123.

List of Figures

Appendix

A. Dissertation Proposal

Please see Appendix A in this document for the full dissertation proposal.

B. Survey Questions

Survey Questions

Note: Questions may be subject to change as the IT artefact develops, but the subject matter will remain the same.

Survey starts with information sheet and consent questionnaire.

Screening Questions 1

1. Are you over the age of 18? {*if No is selected, exited from the survey}*
   - Yes
   - No
2. Have you previously voted in an election in the UK (local or general)? {*if No is selected, exited from the survey}*
   - Yes
   - No

Background Questions

1. Please provide an email address.
    - *Free text*
2. How do you normally vote?
    - In person
    - By post
    - By proxy
3. What is your age bracket?
    - 18-24
    - 25-39
    - 40-59
    - Over 60
4. Are you currently eligible to vote in the UK?
    - Yes
    - No
5. How many times have you voted in a UK election (local or general)
    - Less than 5 times
    - 5-20 times
    - Over 20 times
6. Have you ever heard of electronic voting? {*if Yes go on to question 7, if No go on to question 9}*
    - Yes
    - No
7. Do you agree or disagree with the following statement: Electronic voting is a good thing that should be used in the UK.
    - Strongly agree
    - Agree
    - Neither agree nor disagree
    - Disagree
    - Strongly disagree
8. Would you ever consider voting electronically as opposed to voting by paper? {*if Yes go on to question 10, if No go on to question 9}*
    - Yes
    - No
9. Why would you not consider electronic voting? (Tick all that apply)
    - It feels like too high of a risk
    - I don't understand how electronic voting works
    - I don't understand how electronic voting could be safe
    - Voting in person is an important experience to have
    - I prefer paper voting
    - More research is required before we can do it safely
    - Other (Please specify)
10. Have you ever heard of blockchain? {*if Yes go on to question 11, if No go on to question 13}*
    - Yes
    - No
11. Could you easily describe how blockchain works? {*if Yes go on to question 12, if No go on to question 13}*
    - Yes
    - No
12. Do you know how blockchain could possibly link to electronic voting?
    - Yes
    - No
13. Do you agree or disagree with the following statement: The new requirement to show photographic ID at polling stations in the UK to vote is a good thing.

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly disagree

Screening Questions 2

Participant is prompted to access the testing version of the artefact. The participant then returns to the survey to continue.

What is the code provided at the end of the voting tool?

- *Free text*

Review Questions

These questions will be determined when the IT artefact is fully developed and completed. All questions in this section will pertain to the IT artefact. For example:

- How easy was it to understand how to use the tool?
- How clear was the information provided on how the tool works?
- Would you trust voting with a tool with the features your have seen here?

Concluding Questions

These questions are also subject to the development of the tool but will refer back to previous answers in the survey for example:

- Could you now explain how blockchain works?
- Would you be more open to electronic voting having reviewed this tool?

Appendix C. ETHICAL APPROVAL FORM

Research ethics application form for online programme students

Studies requiring ethics. Any studies involving human participants, personal data, or human tissue require research ethics approval. If you are unsure whether your study requires ethical approval, please use the research ethics decision tool (https://liverpool.onlinesurveys.ac.uk/do-i-need-research-ethics-approval-tool).

Excluded studies. The following studies are outside the scope of a University Research Ethics Committee:
studies that require review by a NHS Research Ethics Committee (http://www.hra-decisiontools.org.uk/ethics/) ; or
studies that require review by an Animal Welfare and Ethical Review Body[i].

Therefore, you may not pursue research which would require approval from these organisations.

Studies outside the UK. Studies conducted outside the UK, local research ethics approval for each country should be sought wherever possible. Please see the research ethics webpages (https://www.liverpool.ac.uk/intranet/research-support-office/research-ethics/international-research/) for guidance on identifying local ethics committees. This process can take a great deal of time. If you think that you will require local ethics approval, speak with your Thesis Supervisor or Dissertation Advisor at the earliest opportunity.

Study permissions. If your study involves other organisations or research sites that require access permission, you will need to seek permission from the relevant organisations involved in the study in order for you to conduct your study. This process may take time so you must plan for this.

Research ethics support. If you have any research ethics questions, please contact ethics@study-online.liverpool.ac.uk.

Research governance requirements.

For any studies involving Sensitive IT Usage[ii], please contact the University's Information Security Officer, Christa Price. You should also discuss this with your Thesis Supervisor or Dissertation Advisor before submitting your research proposal.

All non-desk based studies should be covered by a Health and Safety **risk assessment form** (contact Steve Dunkley for advice on the correct form).

For any studies involving the NHS, please apply for Health Research Authority approval.

University Sponsorship is required for any studies that involve the NHS or healthcare patients overseas. Please visit the Sponsorship webpages (https://www.liverpool.ac.uk/policy-centre/research/sponsorshipofresearch/) or contact sponsor@liverpool.ac.uk for advice on University Sponsorship.

For any studies involving the collection of personal health data, please contact Kevan Ryan for advice on compliance with the Caldicott Principles[iii].

Studies involving any of the following require additional Insurance (https://www.liverpool.ac.uk/intranet/legal/insurance/) confirmation from Mark Neill, and will therefore not be permitted to proceed:
Recruitment of participants in the following groups into interventional studies or observational studies involving the taking of tissue samples (for research purposes)
Children under the age of 5
Pregnant women
Participants who lack the capacity to consent
First in Man Clinical Trials of Investigative Medicinal Products
Clinical Investigations of Medical Devices
Studies including medical intervention involving contraception

Human Health related based Studies taking place at international sites involving clinical or psychological intervention or clinical sampling

Studies undertaken in the UK that involve either prison establishments, or the Ministry of Defence; will need approval from the Ministry of Justice or the Ministry of Defence. It is very unlikely that research of this type would be permitted and you must have a strong case and agreement from your Thesis Supervisor or Dissertation Advisor.

Section 1: Project information

1.1 Title of the research:

Exploring Solutions to Internet Voting in Government Elections in the UK

1.2 Thesis Supervisor(s) or Dissertation Advisor(s) details:

Thesis Supervisor(s) or Dissertation Advisor(s) name:	Andrea Corradini
Thesis Supervisor(s) or Dissertation Advisor(s) email address:	andrea.corradini@liverpool.ac.uk

1.3 Student investigator details:

Student name:	Cheylea Hopkinson
Student programme of study:	MSC Computer Science
Student telephone number:	
Student email address:	C.Z.L.Hopkinson@liverpool.ac.uk

1.4 Are there any other Investigators involved in the study? No

Investigator name:	Investigator role in the study:	Investigator telephone number:	Investigator email address:

1.5 Approximate study dates:

Proposed start date: 05/06/2023
Proposed end date: 15/01/2024

1.6 Please list all the locations where the research will take place[iv]:

Research site:	Individual responsible:	Contact details:
Virtual within the UK	Cheylea Hopkinson	C.Z.L.Hopkinson@liverpool.ac.uk

1.7 Has the study received any external funding? No

Funding body:	
Amount:	
Duration:	
Funding reference number:	

Section 2: Research outside the UK

Research outside the UK should follow the University's procedure for research undertaken outside the UK (https://www.liverpool.ac.uk/intranet/media/livacuk/researchethics/reviewprocedures/Research,outside,the,UK,application,procedure.pdf) . Resources on research at international sites can be

found on the research ethics webpages (https://www.liverpool.ac.uk/intranet/research-support-office/research-ethics/international-research/).

2.1 Will the research take place at a site outside the UK[v]? No
(If the research will not take place outside the UK, please go to question 3.1)

2.2 Is it possible to obtain approval from a local Research Ethics Committee? Choose an item.

If it *is* possible to obtain approval from a local Research Ethics Committee, then you should halt this application form, and apply using the 'Recognition of external approval' application form.

If it is not possible to obtain approval from a local Research Ethics Committee, please answer the questions below.

2.3 Please explain what efforts have been made to identify a local research ethics committee[vi]:

2.4 Please explain whether permission is required from any local organisations or institutions in order to carry out the research?
(*If so, please describe your plans to obtain this approval and provide an indicative timeline for obtaining the approval*)

2.5 Please provide guidance on the local legislative and regulatory environment relevant to research in this setting[vii]:
(*Please provide links to relevant online resources and information. Guidance on potentially relevant legislation in different countries can be found in the* International Compilation of Human Research Standards document)

2.6 Please describe the local cultural practices that are relevant to the conduct of research in this setting[viii]:
(*Please ensure you outline the ways in which your research will address and accommodate these practices*)

2.7 Please provide details of the arrangements to ensure the safety of the researcher[ix]:
(*This should include the safety measures in place to protect participants, as well as other stakeholders who may be involved in the research*)

Section 3: Ethics review routes

3.1 Will the study involve any of the following?

Potentially vulnerable people[x], or potentially vulnerable individuals in a dependent or unequal relationship	No
Children; or adults who may lack the capacity to consent	No
Obtaining consent from a gatekeeper *(For example: a parent, carer, workplace supervisor etc)*	No
The collection of data without written consent from participants	No
Secondary analysis of confidential or sensitive datasets	No
Potentially sensitive topics that may cause distress or embarrassment	No

Topics that raise may require the disclosure of confidential information (criminal activity, child protection etc.)	No
Deception, or misleading participants	No
A physical intervention (exercise, physical contact with people etc.)	No
The administration of substances (food, drink, medication etc.)	No
Human tissue or stem cells	No
Physical risks to the safety of the researcher or the participants	No
Methods where written consent will not be obtained	No
Access to restricted or private data gathered through the internet	No

If you your study involves any of the above categories, then you are likely to require review from the Liverpool Online Research Ethics Committee. You will need to described the associated risks, and how these risks will be managed in section 6 of this form.

Section 4: Description of the research

4.1 Please select which of the following methods/procedures will be used in the study:

Archival research (primary source data held in public or private archives)	☐
Autoethnography	☐
Clinical audit	☐
Focus groups	☐
Human tissue or stem cells	☐
Internet-mediated research (data collected via social media, online chat rooms, private websites etc.)	☐
Interviews	☐
Invasive experiments on human participants (including MRI; X-ray; studies administering food, drink, or medicines; EEGs/ECGs)	☐
Non-invasive experiments on human participants (for example: classroom tests; the administration of tasks to participants etc.)	☐
Observations	☐
Surveys (including questionnaires)	☒
Other	☐

If 'Other' has been selected, please describe the method that will used:

4.2 Please describe the research aims and rationale[xi]:
(*This will be based upon your research proposal*):

Electronic voting is a strongly debated topic and requires continual research and innovation to allow for governments and the public to confidently make decisions on its rollout. The project aims to answer the following questions: Can an internet e-voting system identification check be remote whilst ensuring accuracy and voter anonymity? Would an internet e-voting system compromise the security of the vote casting? Can an internet e-voting system provide two-way transparency between voter and governing body? As part of exploring an electronic solution to voting in the UK, the survey aims to gauge public opinion on the subject itself and levels of confidence in an electronic voting prototype to address these questions.

4.3 Please describe the research design[xii]:
(*This will include the full methodology as outlined in your research proposal*):

There are two parts to the research methodology: a qualitative analysis of existing literature, including case studies and a mixed-method analysis of an IT artefact. The IT artefact will be a prototype of an electronic voting system, which will then undergo quantitative and qualitative analysis through experimental and

running simulations on the IT artefact and collecting feedback through a survey. The combined research will form answers to the questions laid out in the aims and rationale.

Section 5: Recruitment and consent

5.1 Please describe the participant group that you intend to recruit:

Adults over the age of 18 that have previously voted in a local or general election.

5.2 How many participants do you expect to recruit?

171

5.3 How was the number of participants decided upon?

The sample size n was selected based on UK population size p and calculating to a 95% confidence level $Z_{\propto/2}$ and 7.5% margin of error E using the formula below.

$$n = \frac{N \times \frac{{Z_{\propto/2}}^2 \times p \times (1-p)}{E^2}}{N + \frac{{Z_{\propto/2}}^2 \times p \times (1-p)}{E^2} - 1}$$

These parameters were chosen to balance reliable results and feasibility of obtaining the number of responses with the projects constraints.

5.4 Are there any specific participant groups which you aim to include in your sample?

The sample will be expected to cover a wide range of age groups and aim to be proportionally similar to the UK population (Gov.uk, 2018) and scaled to not include under 18s in the sample:
18-24 10.5% (around 18 participants)
25 – 39 25.5% (around 44 participants)
40 – 59 33.2% (around 57 participants)
60+ 30.8% (around 52 participants)

5.5 Are any participant groups to be excluded from this study? No
(If so, please list the groups who will be excluded and explain why they cannot take part in the study)

Anyone under the age of 18 as they are not yet able to vote in government elections in the UK.
Anyone who have not voted in the UK before to limit the participants to those familiar with the current voting process in the UK.

5.6 Describe how potential participants in the study will be identified, approached and recruited:

The survey will be available remotely to any eligible participant and be made with a clear and easy to understand survey interface. Potential participants will be recruited through online environments such as online forums and networks and presented screening questions at the beginning of the survey to determine if they are able to answer the survey. In the unlikely event of low participation, face to face recruitment will be implemented by approaching local groups that contain the target cohorts. To enhance engagement, the information and advertising around the survey will stress the importance of research around the topic.

5.7 Please describe the arrangements for obtaining informed consent from participants:
(*Where written consent will be obtained, a copy of your consent form must be included in your submission*)

Consent will be available at the beginning of the survey and will be required to continue to complete the rest of it.

5.8 Please describe any reimbursements for time and inconvenience, or other forms of compensation that participants may receive[xiii]:
(*Please include a copy of the advertisement material with your submission*):

None

Where written consent will be obtained, please ensure that you use the University's template participant consent form and participant information sheet (https://www.liverpool.ac.uk/intranet/research-support-office/research-ethics/research-ethics-application/).

Section 6: Risk management

In this section, you should reflect on the risks involved in the project.

Please do not write "No risk" or "Not applicable" in the answers below. Applications which do not adequately discuss the risks involved, will be returned to applicants.

While the intention is not to fabricate or overstate potential risks, it should be recognised that all research involving human participants or personal data carries some risk, and applications should contain a constructive reflection on the likelihood and magnitude of risks.

6.1 Please describe the risks to the researcher[xiv]:

As political opinion can be an inflammatory subject, there is a risk the researcher experiences negative reaction towards the survey. Survey answers may not always be useful or honest

6.2 Please describe the risks to the participants[xv]:

As data is collected online it is possible that the data collected breaches confidentiality

6.3 Please describe how the risks will be managed:
(*Please attach a health and safety risk assessment (https://www.liverpool.ac.uk/intranet/safety/guidance/risk-assessment/) if required for any non desk-based research*)

Exposure will be mitigated by correctly storing data, as detailed in section 7. Survey answers will be anonymous. A screening question will be used to identify if a participant has completed the artefact review, strengthening the data quality of the answers. Survey data will be summarised within the dissertation with no raw data.

Section 7: Research data management

Support for your research data management is available from the following sources:
Research data management team (rdm@liverpool.ac.uk)
Information security team (C.J.Price@liverpool.ac.uk)
Data protection team (legal@liverpool.ac.uk)
Records management team (recman@liverpool.ac.uk)

7.1 Please tick the types of data that will be processed during the study, and describe how any data analysis will be carried out:

Audio data	☐
Data associated with human material	☐
Documents and scripts	☐
Geospatial data	☐
Imaging data	☐
Interview transcripts	☐

Online responses	☒
Physiological / biochemical data	☐
Video recordings	☐
Other data type	☐

If 'Other data type' has been selected, please describe the data type that will be processed during the study:

7.2 Please select where the data will be stored during the research project: University network drive (for example, the M Drive or a Departmental Drive)

7.3 *Please describe how the data will be stored securely:*
(Please include details of what the data security arrangements will be):

Survey information will be collected using an online user interface, such as Microsoft Forms. Such services encrypt data at both rest and in transit to keep it protected. https://support.microsoft.com/en-gb/office/security-and-privacy-in-microsoft-forms-7e57f9ba-4aeb-4b1b-9e21-b75318532cd9 Responses will then be downloaded once collected, transferred to the University network drive for storage. Responses held online will be destroyed once transferred.

7.4 During the analysis, the data will be: Fully anonymous
(*For guidance on anonymisation, please see the UK Data Service webpages*)

7.5 Please describe who will have access to this data: Only members of the research team

If individuals external to the research team will have access to the data, please describe how this will be managed:

7.6 How will the data be shared with your Thesis Supervisor or Dissertation Advisor? All data will be stored on a University Network Drive folder that is shared with the Supervisor

If 'Other', please describe how the data will be shared with your Thesis Supervisor or Dissertation Advisor:

7.7 In the written findings for the research, the data will be: Fully anonymised

If the data are to be anonymised, please describe the anonymisation process:

Each response will be given a unique id and any identifiable information will be removed from the dataset.

If the data are to be identifiable, you must ensure that the consent form and participant information sheets explicitly reference the use of identifiable data:

I agree to ensure that the consent form and information sheet explicitly reference the use of identifiable data ☐

7.8 Please select how long the data will be stored for following completion of the study: The data will be deleted upon completion of the study

Please describe the plans for the destruction or long-term storage of the data:

The data will be deleted from the network drive once the dissertation is complete.

7.9: Please describe how the consent forms will be managed: Written consent forms will be digitised and stored electronically alongside the research data for as long as the research data are retained

If 'Other', please describe how the consent forms will be managed:

7.10 Up to what point will participants be able to withdraw their data: Up to the point of anonymisation

If 'Other', please describe the point up to which participants will be able to withdraw their data:

7.11 Will any of the following categories of data be collected during the study:

Racial origin	☐
Political opinions	☐
Ethnic origin	☐
Religious beliefs	☐
Philosophical beliefs	☐
Trade union membership	☐
Genetic data	☐
Biometric data for the purpose of uniquely identifying a person	☐
Data concerning health	☐
Data concerning a person's sex life	☐
Data concerning a person's sexual orientation	☐
Data relating to criminal convictions and offences, or related security measures	☐

If any of the above categories of data will be collected during the study and participants could be identified from this data, then a data protection impact assessment must be completed.

7.12 Will feedback of the findings be given to participants at the participants' request[xvi]? Yes

If feedback of the findings will be given to participants, please describe the process for feeding back the results to participants:

Participants will be advised to contact the researcher if they would like a copy of the written findings.

7.13 Please select how the findings of the research will be disseminated:

Dissertation thesis	☒
Internal report	☐
Conference presentation	☐
Peer reviewed journal	☐
Other	☐

Please describe any ethical issues that arise from this dissemination:

None

7.14: Are there any factors which may compromise the duty of confidentiality towards participants? No

If so, please describe the strategy to manage the factors which could compromise the duty of confidentiality:

7.15 Will personal data be transferred from inside the UK or inside the EU, to a location outside the EU? No

If 'Yes', and personal data will be collected inside the UK or inside the EU, and then transferred outside the EU, you will need to gain explicit consent through the participant consent form:

I understand and agree to obtain explicit consent to transfer the data outside the EU ☐

7.16 It is understood that the Thesis Supervisor or Dissertation Advisor should act as the primary custodian for the data generated by the study: ☒

Section 8: Application sign off declarations

8.1 Are there any declarations of interest (https://www.liverpool.ac.uk/legal/policies/) to disclose in relation to this study? No

If 'Yes', please describe the potential conflict of interest, and how this will be managed:

8.2 Please confirm that you have read and understood the University's Policy on adverse events in research (https://www.liverpool.ac.uk/intranet/research-support-office/research-ethics/review-procedures/) ☒

8.3 Please confirm that you have read and understood the University's Research ethics policy (https://www.liverpool.ac.uk/media/livacuk/researchethics/policyonresearchethics/University,Research,Ethics,policy.pdf): ☒

8.4 Please describe the training in research ethics and research integrity that the Thesis Supervisor or Dissertation Advisor and the Student investigator have undertaken:
(*This should include reference to the University's training in research ethics and research integrity, (*https://www.liverpool.ac.uk/media/livacuk/researchintegrity/traininginresearchintegrity/Accessing,the,Research,Ethics,and,Research,Integrity,courses.pdf*) as well as any relevant training that is specific to the study*)

Thesis Supervisor or Dissertation Advisor training:	
Student investigator training:	Research Ethics in Practice (epideum) Working with human participants Understanding research ethics approval Working ethically in challenging circumstances Working ethically in a global environment

8.5 Checklist of enclosures:

(Have you included the following documents in your submission?)

Participant information sheets:	Yes
Participant consent forms:	Yes
Recruitment advertisement:	Yes
Survey or questionnaire:	Yes
Interview schedule:	Not relevant
Debriefing material:	Not relevant
A protocol for managing distress	Not relevant
Study plan or study protocol:	Not relevant
Evidence of external permissions:	Not relevant
Research data management plan:	Not relevant
Health and safety risk assessment:	Not relevant
Data protection risk assessment:	Yes
Other research tools that will be given to participants:	Not relevant

Academic honesty declaration:	☒

Appendix 1: Literature and guidance notes

University research ethics webpages (https://www.liverpool.ac.uk/intranet/research-support-office/research-ethics/)

Appendix D. CODE USED TO DEVELOP THE IT ARTEFACT

D.1 Application Scripts

D.1.1 app.py

```
#!/usr/bin/python3
# Full version of Electronic Voting Tool (includes Identification)

# General requirements
from datetime import datetime, timedelta
import os
import base64
from socket import gethostname # for PythonAnywhere

# Setup Flask app
from flask import Flask, render_template, request, redirect, url_for,
jsonify
from flask_cors import CORS
app = Flask(__name__, instance_relative_config=True)
CORS(app, resources={r"/storephoto": {"origins":
"http://127.0.0.1:5000/"}})

# Setup blockchain and encryption
import json
from blockchain import Blockchain
from cryptography.fernet import Fernet
from instance.config import encryption_key
blockchain = Blockchain()
app.config.from_pyfile('config.py')
key = encryption_key

# Setup for SQL databases
import sqlite3
from testdetails import myname, myaddress, mypostcode

# Setup for Identification
from identification import Identification
id = Identification()
UPLOAD_FOLDER = 'uploads' # Define a folder to store uploaded images
if not os.path.exists(UPLOAD_FOLDER):
    os.makedirs(UPLOAD_FOLDER)
app.config['UPLOAD_FOLDER'] = UPLOAD_FOLDER

"""
Full Electronic Voting Tool System with biometric and text identifica-
tion using driving
licences.
"""

### Functions for databases ###

def connect_to_database(database_file):
    """Connect to a sqlite database
```

```
    Key arguments
    database_file -- location of sqlite database file
    """
    conn = sqlite3.connect(database_file, isolation_level=None)
    conn.row_factory = sqlite3.Row
    print("Connection successful!")
    return conn

def execute_sql(conn, sql):
    """Execute SQL to a sqlite database

    Key arguments
    conn -- sqlite connection
    sql -- string of sqlite code
    """
    c = conn.cursor()
    c.execute(sql)

def execute_sql_fetch_one(conn, sql):
    """Execute SQL to a sqlite database
    and fetch answer (one answer only)

    Key arguments
    conn -- sqlite connection
    sql -- select string of sqlite code
    """
    c = conn.cursor()
    c.execute(sql)
    result = c.fetchone()
    return result

def execute_sql_fetch_all(conn, sql):
    """Execute SQL to a sqlite database
    and fetch all answers (multiple answers only)

    Key arguments
    conn -- sqlite connection
    sql -- select string of sqlite code
    """
    c = conn.cursor()
    c.execute(sql)
    result = c.fetchall()
    return result

### Encryption Functions ###
def encrypt(key, message: bytes):
    """Encrypt the provided variable

    Key arguments
    key -- key to encrypt with
    message -- the value to be encrypted
    """
    message = message.encode()
    return Fernet(key).encrypt(message)

def decrypt(key, token: bytes):
    """Decrypt the provided variable

    Key arguments
```

```
    key -- key to encrypt with
    message -- the value to be encrypted
    """
    message  = Fernet(key).decrypt(token)
    return message.decode('utf-8')

### Main Application ###
def main():
    """Function that initialises the programme and sets
    up the starting databases

    """

    # Create table for the voters database
    voters = r"databases_test\voters.db"

    # Table that stores information required to identify is a voter is
eligible
    drop_table_voters = """DROP TABLE IF EXISTS voters; """
    create_table_voters = """ CREATE TABLE IF NOT EXISTS voters (
                                id integer PRIMARY KEY,
                                pollstation text,
                                pollnumber integer,
                                name text,
                                address text,
                                postcode text,
                                iseligible integer
                            ); """

    # Insert test voters
    insert_table_voters = """ INSERT INTO voters (id, pollstation, poll-
number, name, address, postcode, iseligible)
                              VALUES
                                (1, 'ABC', 1, 'Charlie Voter (Test)', '1
Example Street', 'ZZ01 000', 1),
                                (2, 'ABC', 2, 'Sam Voter (Test)', '2 Ex-
ample Street', 'ZZ01 000', 1),
                                (3, 'ABC', 3, 'Bailey Voter (Test)', '3
Example Street', 'ZZ01 000', 1),
                                (4, 'ABC', 4, '""" + myname + """', '"""
+ myaddress + """', '""" + mypostcode + """', 1);
                             """

    # Make connection to voters database file
    conn = connect_to_database(voters)
    if conn is not None:
        # Execute required sql
        execute_sql(conn, drop_table_voters)
        execute_sql(conn, create_table_voters)
        execute_sql(conn, insert_table_voters)
        print("Voter database complete.")

    else:
        print("Error, no connection.")

    # Create tables for the votes database
    votes = r"databases_test\votes.db"

    # Table that stores the blockchain
```

```
    drop_table_votes = """DROP TABLE IF EXISTS votes; """
    create_table_votes = """ CREATE TABLE IF NOT EXISTS votes (
                                id integer PRIMARY KEY,
                                block text
                            ); """
    # Table that stores words that cannot be used as secret words
    drop_table_words = """DROP TABLE IF EXISTS words; """
    create_table_words = """ CREATE TABLE IF NOT EXISTS words (
                                id integer PRIMARY KEY,
                                word text,
                                pollstation text
                            ); """
    # Insert banned words
    insert_table_words = """ INSERT INTO words (id, word, pollstation)
                             VALUES
                               (1, 'TEST', 'all'),
                               (2, 'CHARLIE', 'all'),
                               (3, 'VOTER', 'all'),
                               (4, 'SAM', 'all'),
                               (5, 'BAILEY', 'all'),
                               (6, 'EXAMPLE', 'all');
                            """

    # Table that stores basic information about test candidates
    drop_table_candidates = """DROP TABLE IF EXISTS candidates; """
    create_table_candidates = """ CREATE TABLE IF NOT EXISTS candidates
(
                                id integer PRIMARY KEY,
                                candidatename text,
                                candidateparty text
                            ); """

    # Insert test candidates
    insert_table_candidates = """ INSERT INTO candidates (id, candidate-
name, candidateparty)
                              VALUES
                                (1, 'Amanda Candidate', 'Circle Party'),
                                (2, 'Benjamin Candidate', 'Triangle Par-
ty'),
                                (3, 'Chloe Candidate', 'Square Party'),
                                (4, 'David Candidate', 'Pentagon Par-
ty'),
                                (5, 'Emma Candidate', 'Hexagon Party'),
                                (6, 'Frederick Candidate', 'Octogon Par-
ty');
                              """

    # Make connection to voters database file
    conn = connect_to_database(votes)
    if conn is not None:
        # Execute required sql
        execute_sql(conn, drop_table_votes)
        execute_sql(conn, create_table_votes)
        execute_sql(conn, drop_table_words)
        execute_sql(conn, create_table_words)
        execute_sql(conn, insert_table_words)
        execute_sql(conn, drop_table_candidates)
        execute_sql(conn, create_table_candidates)
        execute_sql(conn, insert_table_candidates)
```

```
        print("Votes database complete.")
    else:
        print("Error, no connection.")

    # Add first block to the database so it has a starting point
    firstblock = blockchain.create_block(proof=1, pollstation='none',
secretword='none', candidate='none', previous_hash='0')
    firstblock = str(json.dumps(firstblock))
    insert_first_block = "INSERT INTO votes (block) VALUES ('" +
firstblock + "');"
    execute_sql(conn, insert_first_block)
    conn.close()

# App route for index, an introduction welcome page for survey testing
@app.route("/")
def home():
    return render_template("0_index.html")

# App route for frequently asked questions about the tool and blockchain
@app.route("/faqs")
def faqs():
    return render_template("2_faqs.html")

# Placeholder for providing your poll number or name and address to
check eligibility (must come before ID check)
@app.route("/checkeligibility")
def checkeligibility():
    # Connect to voters and get full list
    voters = r"databases_test\voters.db"
    select_all_voters = "SELECT * FROM voters;"
    conn = connect_to_database(voters)
    result = execute_sql_fetch_all(conn, select_all_voters)
    conn.close
    return render_template("3_checkeligibility.html", test_voters = re-
sult)

# Verify if the person is eligible to vote
@app.route("/verifyeligibility", methods=['GET', 'POST'])
def verifyeligibility():
    # Connect to voters and get eligibility check for person
    voters = r"databases_test\voters.db"
    pollnumber = request.form['tester']
    select_eligibility = "SELECT IsEligible FROM voters WHERE pollsta-
tion || CAST(pollnumber as text) = '" + pollnumber + "';"
    conn = connect_to_database(voters)
    result = execute_sql_fetch_one(conn, select_eligibility)
    conn.close

    pollnumber = encrypt(key, pollnumber) # encrypt for url
    if result[0] == 1:
        # If person is eligible, proceed
        return redirect(url_for('verifyid', pollnumber = pollnumber))
    else:
        # If person is not eligible, redirect
        # For this version of the tool this is an error page as all test
credentials should be eligible
        return redirect(url_for("error"))

# Placeholder for identification process in full version of the artefact
```

```
@app.route("/verifyid/<pollnumber>")
def verifyid(pollnumber):
    # Connect to voters and their details for screen display
    voters = r"databases_test\voters.db"
    pollnumber = decrypt(key, pollnumber) # decrypt for database
    select_voter_details = "SELECT name FROM voters WHERE pollstation ||
CAST(pollnumber as text) = '" + pollnumber + "';"
    conn = connect_to_database(voters)
    result = execute_sql_fetch_one(conn, select_voter_details)
    conn.close

    pollnumber = encrypt(key, pollnumber) # encrypt for url
    return render_template("5_verifyid.html", name = result[0], poll-
number = pollnumber.decode('utf-8'))

# Screen to take photo of driving licence
@app.route("/idphoto/<pollnumber>")
def idphoto(pollnumber):
    return render_template("5a_idphoto.html", pollnumber = pollnumber)

# Store ID photo
@app.route('/storephoto/<pollnumber>', methods=['POST'])
def storephoto(pollnumber):
    imagedata = request.form['imagedata']

    pollnumber = decrypt(key, pollnumber) # decrypt
    pollnumber = encrypt(key, pollnumber) # encrypt

    # Store photo with the encrypted pollnumber
    imagepath = 'idphoto/' + pollnumber.decode('utf-8') + '_idphoto.png'
    imagename = pollnumber.decode('utf-8') + '_idphoto.png'
    with open(imagepath, 'wb') as f:
        f.write(base64.b64decode(imagedata.split(',')[0]))

    return redirect(url_for('checkid', pollnumber = pollnumber.de-
code('utf-8'), imagename = imagename))

# Check Photo
@app.route("/checkid/<pollnumber>/<imagename>", methods=['GET'])
def checkid(pollnumber, imagename):

    # Connect to voters and their get details to compare to ID
    voters = r"databases_test\voters.db"
    pollnumber = decrypt(key, pollnumber) # decrypt for database
    select_voter_name = "SELECT name FROM voters WHERE pollstation ||
CAST(pollnumber as text) = '" + pollnumber + "';"
    select_voter_address = "SELECT address FROM voters WHERE pollstation
|| CAST(pollnumber as text) = '" + pollnumber + "';"
    select_voter_postcode = "SELECT postcode FROM voters WHERE pollsta-
tion || CAST(pollnumber as text) = '" + pollnumber + "';"
    conn = connect_to_database(voters)
    name = execute_sql_fetch_one(conn, select_voter_name)
    address = execute_sql_fetch_one(conn, select_voter_address)
    postcode = execute_sql_fetch_one(conn, select_voter_postcode)
    conn.close
    pollnumber = encrypt(key, pollnumber) # encrypt for url

    name = name[0]
    address = address[0] + postcode[0]
```

```
    # Check identity
    # First check the text on the id card
    imagepath = 'idphoto/' + imagename

    text_result = id.check_identification_text(imagepath, name, address)
    print(text_result)
    if (text_result[0] > 0.5 and text_result[1] > 0.5) or text_result[0]
> 0.75:
        # If passes text check, then moves to photo check
        face_result = id.check_identification_face(imagepath)
        if face_result == "true":
            # If person passes the ID check, then they proceed
            print("passed")
            os.remove(imagepath)
            return jsonify({'status': 'success'})
        elif face_result == "error, face not found":
            print("face not found")
            os.remove(imagepath)
            return jsonify({'status': 'fail'})
        else:
            # If the face check has failed redirect to failure screen
            print("failed face check")
            os.remove(imagepath)
            return jsonify({'status': 'fail'})
    elif text_result[0] == -1: # error, text not found
        # If passes text check, then moves to photo check
        print("text not found")
        os.remove(imagepath)
        return jsonify({'status': 'fail'})
    else:
        print("failed text check")
        os.remove(imagepath)
        return jsonify({'status': 'fail'})

# Screen for passed ID check
@app.route("/passedidcheck/<pollnumber>")
def passedidcheck(pollnumber):
    return render_template("5b_idphoto_pass.html", pollnumber = poll-
number)

# Screen for failed ID check
@app.route("/failedidcheck/<pollnumber>")
def failedidcheck(pollnumber):
    return render_template("5c_idphoto_fail.html", pollnumber = poll-
number)

# Screen to enter secret word
@app.route("/enterword/<pollnumber>")
def enterword(pollnumber):
    return render_template("6_enterword.html", pollnumber = pollnumber)

# Submission route when entering a secret word
@app.route("/enterwordcheck/<pollnumber>", methods=['GET', 'POST'])
def enterwordcheck(pollnumber):
    #  Connect to votes database to check if secret word has been used
    votes = r"databases_test\votes.db"
    secretword = request.form['sword'].upper()
    pollnumber = pollnumber.encode()
```

```
    pollnumber = decrypt(key, pollnumber) # decrypt for database
    pollstation = pollnumber[:3] # extract poll station from poll number
    count_matching_words = "SELECT COUNT(*) FROM words w WHERE pollsta-
tion IN ('all', '"+ pollstation +"') AND word = '" + secretword + "';"
    conn = connect_to_database(votes)
    result = execute_sql_fetch_one(conn, count_matching_words)
    conn.close

    pollnumber = encrypt(key, pollnumber) # encrypt for url
    secretword = encrypt(key, secretword) # encrypt for url
    if result[0] == 0:
        # If word has not been used, proceed to vote page
        return redirect(url_for('vote', pollnumber = pollnumber, secret-
word = secretword))
    else:
        # If word has been used before, error and redirect to page indi-
cating to try again
        return redirect(url_for('enterworderror', pollnumber = poll-
number))

# Screen to enter secret word when previous word cannot be used with er-
ror message
@app.route("/enterworderror/<pollnumber>")
def enterworderror(pollnumber):
    errormessage = 'The word you have entered cannot be used. Please se-
lect another word.'
    return render_template("6_enterword.html", pollnumber = pollnumber,
errormessage = errormessage)

# Screen to vote
@app.route("/vote/<pollnumber>/<secretword>")
def vote(pollnumber, secretword):
    # Connect to voters database to get list of candidates to vote for
    voters = r"databases_test\votes.db"
    select_all_candidates = "SELECT * FROM candidates;"
    conn = connect_to_database(voters)
    result = execute_sql_fetch_all(conn, select_all_candidates)
    conn.close
    return render_template("7_vote.html", candidates = result, poll-
number = pollnumber, secretword = secretword)

# Submission route when submitting vote
@app.route('/submitvote/<pollnumber>/<secretword>', methods=['GET',
'POST'])
def submitvote(pollnumber, secretword):
    # Connect to votes database to get last block
    votes = r"databases_test\votes.db"
    select_last_block = "SELECT block FROM votes v JOIN (SELECT MAX(id)
id FROM votes) max ON max.id = v.id"
    conn = connect_to_database(votes)
    previous_block = execute_sql_fetch_all(conn, select_last_block)

    # Loads the different parts of the blockchain block
    for row in previous_block:
        previous_block = json.loads(row[0])
    previous_proof = previous_block['proof']

    # Get required block variables
    proof = blockchain.proof_of_work(previous_proof)
```

```
    previous_hash = blockchain.hash(previous_block)
    candidate = request.form['candidates']
    pollnumber = decrypt(key, pollnumber.encode())
    secretword = decrypt(key, secretword)
    pollstation = ''.join(filter(str.isalpha, pollnumber))

    # Mine new block
    block = blockchain.create_block(proof, pollstation, secretword, can-
didate, previous_hash)
    block = str(json.dumps(block))

    # Insert block and used word into votes database
    try:
        insert_new_block = "INSERT INTO votes (block) VALUES ('" + block
+ "');"
        insert_used_word = "INSERT INTO words (word, pollstation) VALUES
('" + secretword + "', '" + pollstation + "');"
        execute_sql(conn, insert_new_block)
        execute_sql(conn, insert_used_word)
        conn.commit()
        conn.close
    except:
        return redirect("error.html")

    # Person marked as ineligible to vote once vote is committed
    voters = r"databases_test\voters.db"
    mark_ineligible = "UPDATE voters SET IsEligible = 0 FROM (SELECT *
FROM voters) voterslist WHERE voters.pollstation ||
CAST(voters.pollnumber as text) = '" + pollnumber + "';"
    conn2 = connect_to_database(voters)
    execute_sql(conn2, mark_ineligible)
    conn.commit()
    conn.close

    return render_template("8_complete.html")

# Screen to request pollstation and secret word to verify vote
@app.route("/verify")
def verify():
    return render_template("9_verify.html")

# Submission route when requesting verification
@app.route("/fetchvote/", methods=['GET', 'POST'])
def fetchvote():
    # Connect to votes database to get who person voted for
    secretword = request.form['sword'].upper()
    pollstation = request.form['pollstation'].upper()
    voter = pollstation + secretword
    votes = r"databases_test\votes.db"
    select_vote = "SELECT block FROM votes v WHERE JSON_EXTRACT(block,
'$.voter') = '" + voter + "';"
    conn = connect_to_database(votes)
    voteblock = execute_sql_fetch_all(conn, select_vote)
    conn.close()

    # If vote is found
    if voteblock:
        # Loads the different parts of the blockchain block
        for row in voteblock:
```

```
            voteblock = json.loads(row[0])

        # Calculate if vote is in expiration period
        candidate = voteblock['candidate']
        timestamp = voteblock['timestamp']
        currenttime = datetime.now()
        timelimit = (datetime.strptime(timestamp,
"%Y-%m-%d %H:%M:%S.%f") + timedelta(minutes=5))

        if currenttime >= timelimit:
            # If too much time has passed, the user is notified this has
expired
            errormessage = 'Time to verify vote has expired.'
            candidate = 'Unable to view candidate.'
            return render_template("10_seevote.html", candidate = candi-
date, errormessage = errormessage)
        else:
            # If still within the time frame, user is shown their vote
            errormessage = ''
            if len(candidate) == 0:
                candidate = 'You registered your vote as a non vote.'
            else:
                candidate = 'You voted for ' + candidate + '.'
            return render_template("10_seevote.html", candidate = candi-
date, errormessage = errormessage)

    # If vote cannot be found
    else:
        errormessage = 'Word and polling station did not find a match.'
        candidate = 'Unable to view candidate.'
        return render_template("10_seevote.html", candidate = candidate,
errormessage = errormessage)

# Error page
@app.route("/error")
def error():
    return render_template("error.html")

# Initialise
if __name__ == '__main__':
    main()
    # If statement to prevent run when hosting in PythonAnywhere
    if 'liveconsole' not in gethostname():
        app.run(debug=True)
```

D.1.2 app_test.py

```
#!/usr/bin/python3
# Test version of Electronic Voting Tool (does not include Identifica-
tion)
"""
Test version of the Electronic Voting Tool System with biometric and
text identification using driving
licences.
This application is currently hosted at: https://www.selfverification-
electronicvotingtool.co.uk/
"""
```

```
# General requirements
from datetime import datetime, timedelta
from socket import gethostname # for PythonAnywhere

# Setup Flask app
from flask import Flask, render_template, request, redirect, url_for
from flask_cors import CORS
app = Flask(__name__, instance_relative_config=True)
CORS(app, resources={r"/storephoto": {"origins":
"http://127.0.0.1:5000/"}})

# Setup blockchain and encryption
import json
from blockchain import Blockchain
from cryptography.fernet import Fernet
from instance.config import encryption_key
blockchain = Blockchain()
app.config.from_pyfile('config.py')
key = encryption_key

# Setup for SQL databases
import sqlite3


# Functions for databases

def connect_to_database(database_file):
    """Connect to a sqlite database

    Key arguments
    database_file -- location of sqlite database file
    """
    conn = sqlite3.connect(database_file, isolation_level=None)
    conn.row_factory = sqlite3.Row
    print("Connection successful!")
    return conn

def execute_sql(conn, sql):
    """Execute SQL to a sqlite database

    Key arguments
    conn -- sqlite connection
    sql -- string of sqlite code
    """
    c = conn.cursor()
    c.execute(sql)

def execute_sql_fetch_one(conn, sql):
    """Execute SQL to a sqlite database
    and fetch answer (one answer only)

    Key arguments
    conn -- sqlite connection
    sql -- select string of sqlite code
    """
    c = conn.cursor()
    c.execute(sql)
    result = c.fetchone()
    return result
```

```
def execute_sql_fetch_all(conn, sql):
    """Execute SQL to a sqlite database
    and fetch all answers (multiple answers only)

    Key arguments
    conn -- sqlite connection
    sql -- select string of sqlite code
    """
    c = conn.cursor()
    c.execute(sql)
    result = c.fetchall()
    return result

def encrypt(key, message: bytes):
    """Encrypt the provided variable

    Key arguments
    key -- key to encrypt with
    message -- the value to be encrypted
    """
    message = message.encode()
    return Fernet(key).encrypt(message)

def decrypt(key, token: bytes):
    """Decrypt the provided variable

    Key arguments
    key -- key to encrypt with
    message -- the value to be encrypted
    """
    message  = Fernet(key).decrypt(token)
    return message.decode('utf-8')

def main():
    """Function that initialises the programme and sets
    up the starting databases

    """

    # Create table for the voters database
    voters = r"databases_test\voters.db"

    # Table that stores information required to identify is a voter is
eligible
    drop_table_voters = """DROP TABLE IF EXISTS voters; """
    create_table_voters = """ CREATE TABLE IF NOT EXISTS voters (
                                id integer PRIMARY KEY,
                                pollstation text,
                                pollnumber integer,
                                name text,
                                address text,
                                postcode text,
                                iseligible integer
                            ); """

    # Insert test voters
    insert_table_voters = """ INSERT INTO voters (id, pollstation, poll-
number, name, address, postcode, iseligible)
```

```
                                VALUES
                                  (1, 'ABC', 1, 'Charlie Voter (Test)', '1
Example Street', 'ZZ01 000', 1),
                                  (2, 'ABC', 2, 'Sam Voter (Test)', '2 Ex-
ample Street', 'ZZ01 000', 1),
                                  (3, 'ABC', 3, 'Bailey Voter (Test)', '3
Example Street', 'ZZ01 000', 1);
                                """

    # Make connection to voters database file
    conn = connect_to_database(voters)
    if conn is not None:
        # Execute required sql
        execute_sql(conn, drop_table_voters)
        execute_sql(conn, create_table_voters)
        execute_sql(conn, insert_table_voters)
        print("Voter database complete.")

    else:
        print("Error, no connection.")

    # Create tables for the votes database
    votes = r"databases_test\votes.db"

    # Table that stores the blockchain
    drop_table_votes = """DROP TABLE IF EXISTS votes; """
    create_table_votes = """ CREATE TABLE IF NOT EXISTS votes (
                                id integer PRIMARY KEY,
                                block text
                            ); """
    # Table that stores words that cannot be used as secret words
    drop_table_words = """DROP TABLE IF EXISTS words; """
    create_table_words = """ CREATE TABLE IF NOT EXISTS words (
                                id integer PRIMARY KEY,
                                word text,
                                pollstation text
                            ); """
    # Insert banned words
    insert_table_words = """ INSERT INTO words (id, word, pollstation)
                                VALUES
                                  (1, 'TEST', 'all'),
                                  (2, 'CHARLIE', 'all'),
                                  (3, 'VOTER', 'all'),
                                  (4, 'SAM', 'all'),
                                  (5, 'BAILEY', 'all'),
                                  (6, 'EXAMPLE', 'all');
                                """

    # Table that stores basic information about test candidates
    drop_table_candidates = """DROP TABLE IF EXISTS candidates; """
    create_table_candidates = """ CREATE TABLE IF NOT EXISTS candidates
(
                                id integer PRIMARY KEY,
                                candidatename text,
                                candidateparty text
                            ); """

    # Insert test candidates
```

```
    insert_table_candidates = """ INSERT INTO candidates (id, candidate-
name, candidateparty)
                                VALUES
                                  (1, 'Amanda Candidate', 'Circle Party'),
                                  (2, 'Benjamin Candidate', 'Triangle Par-
ty'),
                                  (3, 'Chloe Candidate', 'Square Party'),
                                  (4, 'David Candidate', 'Pentagon Par-
ty'),
                                  (5, 'Emma Candidate', 'Hexagon Party'),
                                  (6, 'Frederick Candidate', 'Octogon Par-
ty');
                                """

    # Make connection to voters database file
    conn = connect_to_database(votes)
    if conn is not None:
        # Execute required sql
        execute_sql(conn, drop_table_votes)
        execute_sql(conn, create_table_votes)
        execute_sql(conn, drop_table_words)
        execute_sql(conn, create_table_words)
        execute_sql(conn, insert_table_words)
        execute_sql(conn, drop_table_candidates)
        execute_sql(conn, create_table_candidates)
        execute_sql(conn, insert_table_candidates)
        print("Votes database complete.")
    else:
        print("Error, no connection.")

    # Add first block to the database so it has a starting point
    firstblock = blockchain.create_block(proof=1, pollstation='none',
secretword='none', candidate='none', previous_hash='0')
    firstblock = str(json.dumps(firstblock))
    insert_first_block = "INSERT INTO votes (block) VALUES ('" +
firstblock + "');"
    execute_sql(conn, insert_first_block)
    conn.close()

# App route for index, an introduction welcome page for survey testing
@app.route("/")
def home():
    return render_template("1_indextest.html")

# App route for frequently asked questions about the tool and blockchain
@app.route("/faqs")
def info():
    return render_template("2_faqs.html")

# Placeholder for providing your poll number or name and address to
check eligibility (must come before ID check)
@app.route("/checkeligibility")
def checkeligibility():
    # Connect to voters and get full list
    voters = r"databases_test\voters.db"
    select_all_voters = "SELECT * FROM voters;"
    conn = connect_to_database(voters)
    result = execute_sql_fetch_all(conn, select_all_voters)
    conn.close
```

```
    return render_template("4_checkeligibilitytest.html", test_voters =
result)

# Verify if the person is eligible to vote
@app.route("/verifyeligibility", methods=['GET', 'POST'])
def verifyeligibility():
    # Connect to voters and get eligibility check for person
    voters = r"databases_test\voters.db"
    pollnumber = request.form['tester']
    select_eligibility = "SELECT IsEligible FROM voters WHERE pollsta-
tion || CAST(pollnumber as text) = '" + pollnumber + "';"
    conn = connect_to_database(voters)
    result = execute_sql_fetch_one(conn, select_eligibility)
    conn.close

    pollnumber = encrypt(key, pollnumber) # encrypt for url

    if result[0] == 1:
        # If person is eligible, proceed
        return redirect(url_for('verifyid', pollnumber = pollnumber))
    else:
        # If person is not eligible, redirect
        # For this version of the tool this is an error page as all test
credentials should be eligible
        return redirect("error.html")


# Placeholder for identification process in full version of the artefact
@app.route("/verifyid/<pollnumber>")
def verifyid(pollnumber):
    # Connect to voters and their details for screen display
    voters = r"databases_test\voters.db"
    pollnumber = decrypt(key, pollnumber) # decrypt for database
    select_voter_details = "SELECT name FROM voters WHERE pollstation ||
CAST(pollnumber as text) = '" + pollnumber + "';"
    conn = connect_to_database(voters)
    result = execute_sql_fetch_one(conn, select_voter_details)
    conn.close

    pollnumber = encrypt(key, pollnumber) # encrypt for url

    return render_template("5_verifyidtest.html", name = result[0],
pollnumber = pollnumber.decode('utf-8'))

# Screen to enter secret word
@app.route("/enterword/<pollnumber>")
def enterword(pollnumber):
    return render_template("6_enterword.html", pollnumber = pollnumber)

# Submission route when entering a secret word
@app.route("/enterwordcheck/<pollnumber>", methods=['GET', 'POST'])
def enterwordcheck(pollnumber):
    #  Connect to votes database to check if secret word has been used
    votes = r"databases_test\votes.db"
    secretword = request.form['sword'].upper()
    pollnumber = pollnumber.encode()
    pollnumber = decrypt(key, pollnumber) # decrypt for database
    pollstation = pollnumber[:3] # extract poll station from poll number
```

```
    count_matching_words = "SELECT COUNT(*) FROM words w WHERE pollsta-
tion IN ('all', '"+ pollstation +"') AND word = '" + secretword + "';"
    conn = connect_to_database(votes)
    result = execute_sql_fetch_one(conn, count_matching_words)
    conn.close

    pollnumber = encrypt(key, pollnumber) # encrypt for url
    secretword = encrypt(key, secretword) # encrypt for url
    if result[0] == 0:
        # If word has not been used, proceed to voe page
        return redirect(url_for('vote', pollnumber = pollnumber, secret-
word = secretword))
    else:
        # If word has been used before, error and redirect to page indi-
cating to try again
        return redirect(url_for('enterworderror', pollnumber = poll-
number))

# Screen to enter secret word when previous word cannot be used with er-
ror message
@app.route("/enterworderror/<pollnumber>")
def enterworderror(pollnumber):
    errormessage = 'The word you have entered cannot be used. Please se-
lect another word.'
    return render_template("6_enterword.html", pollnumber = pollnumber,
errormessage = errormessage)

# Screen to vote
@app.route("/vote/<pollnumber>/<secretword>")
def vote(pollnumber, secretword):
    # Connect to voters database to get list of candidates to vote for
    voters = r"databases_test\votes.db"
    select_all_candidates = "SELECT * FROM candidates;"
    conn = connect_to_database(voters)
    result = execute_sql_fetch_all(conn, select_all_candidates)
    conn.close
    return render_template("7_vote.html", candidates = result, poll-
number = pollnumber, secretword = secretword)

# Submission route when submitting vote
@app.route('/submitvote/<pollnumber>/<secretword>', methods=['GET',
'POST'])
def submitvote(pollnumber, secretword):
    # Connect to votes database to get last block
    votes = r"databases_test\votes.db"
    select_last_block = "SELECT block FROM votes v JOIN (SELECT MAX(id)
id FROM votes) max ON max.id = v.id"
    conn = connect_to_database(votes)
    previous_block = execute_sql_fetch_all(conn, select_last_block)

    # Loads the different parts of the blockchain block
    for row in previous_block:
        previous_block = json.loads(row[0])
    previous_proof = previous_block['proof']

    # Get required block variables
    proof = blockchain.proof_of_work(previous_proof)
    previous_hash = blockchain.hash(previous_block)
    candidate = request.form['candidates']
```

```
    pollnumber = decrypt(key, pollnumber.encode())
    secretword = decrypt(key, secretword)
    pollstation = ''.join(filter(str.isalpha, pollnumber))

    # Mine new block
    block = blockchain.create_block(proof, pollstation, secretword, can-
didate, previous_hash)
    block = str(json.dumps(block))

    # Insert block and used word into votes database
    insert_new_block = "INSERT INTO votes (block) VALUES ('" + block +
"');"
    insert_used_word = "INSERT INTO words (word, pollstation) VALUES ('"
+ secretword + "', '" + pollstation + "');"
    execute_sql(conn, insert_new_block)
    execute_sql(conn, insert_used_word)
    conn.commit()
    # In full version the person would be marked as ineligible to vote
once vote is committed
    conn.close
    return render_template("8_complete.html")

# Screen to request pollstation and secret word to verify vote
@app.route("/verify")
def verify():
    return render_template("9_verify.html")

# Submission route when requesting verification
@app.route("/fetchvote/", methods=['GET', 'POST'])
def fetchvote():
    # Connect to votes database to get who person voted for
    secretword = request.form['sword'].upper()
    pollstation = request.form['pollstation'].upper()
    voter = pollstation + secretword
    votes = r"databases_test\votes.db"
    select_vote = "SELECT block FROM votes v WHERE JSON_EXTRACT(block,
'$.voter') = '" + voter + "';"
    conn = connect_to_database(votes)
    voteblock = execute_sql_fetch_all(conn, select_vote)
    conn.close()

    # If vote is found
    if voteblock:
        # Loads the different parts of the blockchain block
        for row in voteblock:
            voteblock = json.loads(row[0])

        # Calculate if vote is in expiration period
        candidate = voteblock['candidate']
        timestamp = voteblock['timestamp']
        currenttime = datetime.now()
        timelimit = (datetime.strptime(timestamp,
"%Y-%m-%d %H:%M:%S.%f") + timedelta(minutes=5))

        if currenttime >= timelimit:
            # If too much time has passed, the user is notified this has
expired
            errormessage = 'Time to verify vote has expired.'
            candidate = 'Unable to view candidate.'
```

```
            return render_template("10_seevotetest.html", candidate =
candidate, errormessage = errormessage)
        else:
            # If still within the time frame, user is shown their vote
            errormessage = ''
            if len(candidate) == 0:
                candidate = 'You registered your vote as a non vote.'
            else:
                candidate = 'You voted for ' + candidate + '.'
            return render_template("10_seevotetest.html", candidate =
candidate, errormessage = errormessage)

    # If vote cannot be found
    else:
        errormessage = 'Word and polling station did not find a match.'
        candidate = 'Unable to view candidate.'
        return render_template("10_seevotetest.html", candidate = candi-
date, errormessage = errormessage)

# Error page
@app.route("/error")
def error():
    return render_template("error.html")

# Initialise
if __name__ == '__main__':
    main()
    # If statement to prevent run when hosting in PythonAnywhere
    if 'liveconsole' not in gethostname():
        app.run(debug=True)
```

D.1.3 blockchain.py

```
#!/usr/bin/python3
# Python program to create Blockchain
"""
Source: https://www.geeksforgeeks.org/create-simple-blockchain-using-py-
thon/
"""

# Imports
import datetime # for timestamp
import hashlib # hash calculation for block fingerprints
import json # to store data in blockchain

class Blockchain:

    def __init__(self):
        """Create first block and set its hash to "0"
        """
        self.chain = []
        self.create_block(proof=1, pollstation='none', secret-
word='none', candidate='none', previous_hash='0')

    def create_block(self, proof, pollstation, secretword, candidate,
previous_hash):
        """Create a block to add to the chain
```

```
        Key arguments
        proof --
        pollstation --
        secretword --
        candidate --
        previous_hash --
        """
        voter = pollstation + secretword
        block = {'index': len(self.chain) + 1,
                 'timestamp': str(datetime.datetime.now()),
                 'proof': proof,
                 'voter': voter,
                 'candidate': candidate,
                 'previous_hash': previous_hash}
        self.chain.append(block)
        return block

    def return_previous_block(self):
        """Display previous block
        """
        return self.chain[-1]

    def proof_of_work(self, previous_proof):
        """Proof of work to mine block

        Key arguments
        previous_proof --
        """
        new_proof = 1
        check_proof = False

        while check_proof is False:
            hash_operation = hashlib.sha256(
                str(new_proof**2 - previous_proof**2).en-
code()).hexdigest()
            if hash_operation[:5] == '00000':
                check_proof = True
            else:
                new_proof += 1

        return new_proof

    def hash(self, block):
        """Has calculation for block

        Key arguments
        block --
        """
        encoded_block = json.dumps(block, sort_keys=True).encode()
        return hashlib.sha256(encoded_block).hexdigest()

    def chain_valid(self, chain):
        """Validate chain

        Key arguments
        chain -- a blockchain to check the validation of
        """
        previous_block = chain[0]
        block_index = 1
```

```
        while block_index < len(chain):
            block = chain[block_index]
            if block['previous_hash'] != self.hash(previous_block):
                return False

            previous_proof = previous_block['proof']
            proof = block['proof']
            hash_operation = hashlib.sha256(
                str(proof**2 - previous_proof**2).encode()).hexdigest()

            if hash_operation[:5] != '00000':
                return False
            previous_block = block
            block_index += 1

        return True
```

D.1.4 identification.py

```
#!/usr/bin/python3
# Python program to create Blockchain

# Imports
import cv2
import face_recognition
import datetime as dt
import pytesseract
from PIL import Image
from difflib import SequenceMatcher

"""
Class containing functions for the biometric and text identification
check.
Functions accept an image path to use for identification.
Sources:
https://realpython.com/face-recognition-with-python/
https://medium.com/@pawan329/ocr-extract-text-from-image-in-8-easy-
steps-3113a1141c34

"""

class Identification:

    # Set up text recognition for the ID
    def check_identification_text(self, imagepath, name, address):
        """Scan an image to identify any text and compare it to a name
and address
        Designed to work only with a provisional or full UK driving li-
cence.

        Function will return a list with two numbers eg. [1,1] with the
first being the
        text similarity percentage to the name and second to the ad-
dress.
        If [-1,-1] is returned then an error has occured.

        Key arguments
```

```
        imagepath -- path for the image of the provisional or full UK
driving licence eg. idphoto/image.png
        name -- name for the person to be id checked
        address -- address for the person to be id checked
        """

        # Open the image to use
        image = Image.open(imagepath)

        # Use Tesseract to extract text from the image
        pytesseract.pytesseract.tesseract_cmd = r"C:\Program Files\Tes-
seract-OCR\tesseract.exe"
        text = pytesseract.image_to_string(image)

        # Provisional or full UK driving licence take up multiple lines
        # Split the text string of new lines into sections
        text_split = text.splitlines()

        # Try to extract full name
        try:
            # First name should be on the third line and last name on
the second line
            id_name = text_split[3] + text_split[2] # Concatenate name
        except:
            # If an error has occured then usually an image without text
is being used
            name_similarity_ratio = -1 # set to -1 to record it as an
error
            address_similarity_ratio = -1 # set to -1 to record it as an
error
            return name_similarity_ratio, address_similarity_ratio

        # Clean up the name found on the ID licence to improve similar-
ity check
        id_name = id_name.replace(" ","").replace(",","").upper() # Re-
move spaces, commas and capitalise
        id_name = id_name.re-
place("MR","").replace("MRS","").replace("MISS","").replace("DR","").rep
lace("REV","").replace("MX","") # Strip titles

        # Clean up the comparison name given to the function to improve
similarity check
        name = name.replace(" ","").replace(",","").upper() # Remove
spaces, commas and capitalise

        # Try to extract address
        try:
            # Address should begin on the 12th line of the id text
            id_address = text_split[12]
        except:
            # If an error has occured then usually an image without text
is being used
            name_similarity_ratio = -1 # set to -1 to record it as an
error
            address_similarity_ratio = -1 # set to -1 to record it as an
error
            return name_similarity_ratio, address_similarity_ratio
```

```
        # Some addresses go over more than one line, this is indicated
by a comma
        # Check if there is a comma at the end and concatenate the next
two or three lines
        # if so
        if id_address.endswith(",") or id_address.endswith("."): # Add
next line if over 2 lines
            id_address = id_address + text_split[13]
            if id_address.endswith(",") or id_address.endswith("."): #
Add next line if over 3 lines
                id_address = id_address + text_split[14]

        # Clean up the address found on the ID licence to improve simi-
larity check
        id_address = id_address.replace(" ","").replace(",","").upper()
# Remove spaces, commas and capitalise

        # Clean up the comparison address given to the function to im-
prove similarity check
        address = address.replace(" ","").replace(",","").upper() # Re-
move spaces, commas and capitalise

        # Run the SequenceMatcher to calculate the similarity ratios for
name and address
        name_similarity_ratio = SequenceMatcher(None, id_name, name).ra-
tio()
        address_similarity_ratio = SequenceMatcher(None, id_address, ad-
dress).ratio()

        # Return the similarities as a list eg. [1,1]
        return name_similarity_ratio, address_similarity_ratio

    def check_identification_face(self, image_path):
        """Scan an image to identify a single face and compare it to a
live face in the webcam.
        Can work with any image.

        Function will return a "true" or "false" result to indicate if
the face in each image
        matches each other.

        Key arguments
        image_path -- path for the image eg. idphoto/image.png
        """

        # Try to recognise a face in the provided image
        try:
            # Load the image file
            face = face_recognition.load_image_file(image_path)
            # Encode image for comparison
            known_encoding = face_recognition.face_encodings(face)[0]
        except:
            # If error, this means a face has not been found
            matched = "error, face not found"
            return matched

        # Once a face has been recognised in the provided image, the
webcam
        # is opened to live check the user.
```

```
        # Open the webcam
        video_capture = cv2.VideoCapture(0)
        # Calculate the start time for future time out if a face cannot
be found
        # This is to give a period of time for the person to adjust
themselves
        # if they were unprepared for the webcame
        starttime = dt.datetime.now()

        # Loop through captures until a face and match is found or time
out after
        # two minutes

        while True:
            # Capture each frame
            ret, frame = video_capture.read()

            # Find all face locations and encodings in the current frame
            face_locations = face_recognition.face_locations(frame)
            face_encodings = face_recognition.face_encodings(frame,
face_locations)

            # Check if captured face matches the provided image
            for (top, right, bottom, left), face_encoding in
zip(face_locations, face_encodings):
                # Add results to matches variable
                matches = face_recognition.compare_faces([known_encod-
ing], face_encoding)
                print("no match yet")
                # If a true match is found
                if True in matches:
                    # Set to true
                    matched = "true"
                    # Close webcam
                    video_capture.release()
                    # Return result
                    return matched


            # Stop trying after 2 minutes
            # Set 2 minute change
            time_change = dt.timedelta(minutes=0.4)
            # Set the stop time to start time plus 2 minutes

            stop_time = starttime + time_change
            # If time exceeded the stop time, the result is returned as
false
            if stop_time < dt.datetime.now():
                # Set to false
                matched = "false"
                # Close webcam
                video_capture.release()
                print("time expired")
                # Return result
                return matched
```

D.1.5 README.md

````
# Internet Electronic Voting Tool with Biometric and Text Identification
and Self Verification

This repository contains code for an internet electronic voting tool
that uses a biometric and text identification system and a secret word
self verification system. It is a prototype design for a potential vot-
ing model that could be used in UK government elections.

This project is for MSci in Computer Science at University of Liverpool.

Author: Cheylea Hopkinson

## Python Version
This project requires Python 3.9.12.

# Directory
The `instance` and `idphoto` folders may not be found in this reposi-
tiory and will need to be created upon download. More information under
installation.

```
C:.
├───__init__.py
├───app_test.py
├───app.py
├───blockchain.py
├───identification.py
├───LICENSE
├───README.md
├───requirements.txt
├───databases_test
│   ├───voters.db
│   └───votes.db
├───idphoto
├───instance
├───static
├───templates
└───test
    ├───results
    ├───test_images
    ├───blockchain_test.py
    └───identification_test.py
```

# Installation

## Step One
Use the package manager [pip](https://pip.pypa.io/en/stable/) to install
the dependencies.

```
python -m pip install -r requirements.txt
```
You will also need to download and install [Tesser-
act](https://github.com/UB-Mannheim/tesseract/wiki).

## Step Two
````

Create the folder `instance` if required in the repository as indicated in the directory. Create a file caled `config.py`. Copy and paste and save into it the below:

```python
SECRET_KEY = ''
encryption_key = ''
```
Add your own keys into the strings to run the programme.

Step Three
Create the folder `idphoto` if required in the repository as indicated in the directory. Leave empty.

Usage

There are two versions of this tool in the repository. The "test" version `app_test.py` that skips the biometric identification and the version that is the complete tool `app.py`.

Step One
Run either `app.py` or `app_test.py` to run the application. You can configure the port at the bottom of the `app_test.py`. For example:

```python
# Before
if __name__ == '__main__':
    main()
    # If statement to prevent run when hosting in PythonAnywhere
    if 'liveconsole' not in gethostname():
        app.run()

# After
if __name__ == '__main__':
    main()
    # If statement to prevent run when hosting in PythonAnywhere
    if 'liveconsole' not in gethostname():
        app.run(debug=True, port = 8000)
```

Then, if port is set to `8000`, navigate to http://127.0.0.1:8000 to view and click through the application to use it.

Step Two - app.py only
`app.py` will require at least one test credential which is set up in the app.py script:

```python
from testdetails import myname, myaddress, mypostcode

...

# Insert test voters
insert_table_voters = """ INSERT INTO voters (id, pollstation, poll-
number, name, address, postcode, iseligible)
                          VALUES
                            (1, 'ABC', 1, 'Charlie Voter (Test)', '1 Ex-
ample Street', 'ZZ01 000', 1),
```

```
                            (2, 'ABC', 2, 'Sam Voter (Test)', '2 Example
Street', 'ZZ01 000', 1),
                            (3, 'ABC', 3, 'Bailey Voter (Test)', '3 Ex-
ample Street', 'ZZ01 000', 1),
                            (4, 'ABC', 4, '""" + myname + """', '""" +
myaddress + """', '""" + mypostcode + """', 1);
```

Create a file in the root called `testdetails.py` and paste your test details to compare to a real or generated id:

``` python

# My Address
myname = 'John Smith' # full name
myaddress = '1 Test Street' # address without postcode
mypostcode = 'AA00 0AA' # postcode

```

Step Three - app.py only
You may get an error if your tesseract install is not located at `r"C:\Program Files\Tesseract-OCR\tesseract.exe"`. Ensure you have downloaded and installed [Tesseract](https://github.com/UB-Mannheim/) as mentioned in installed. Then you may need to correct the script in `identification.py` to the correct directory:

``` python
# Use Tesseract to extract text from the image
pytesseract.pytesseract.tesseract_cmd = r"C:\Program Files\Tesseract-
OCR\tesseract.exe"
text = pytesseract.image_to_string(image)
```

Testing

Identification
`identification_test.py` is a file for looping through the text and face recognition tools to check their results from a provided folder of images. Load your images into the text_images folder.
Open the folder in file explorer and right click to open terminal. Type in the following

``` bash
dir /b > filenames.txt
```

This will create a file in the images folder that is used in the test module to load in the file path for the images. To prevent any images uploading to git, add these file names to your `.gitignore` file.

There are example results provided in the folder `test/results` which can be used to calculate the results by running the `identification_test.py` file. To refresh the results, uncomment where indicated.

Blockchain
`blockchain_test.py` is a file for looping through test blockchains with added interference. This is to test the chain valid function and to ensure altered blocks would be identified.

```
There are example results provided in the folder `test/results` which
can be used to calculate the results by running the `blockchain_test.py`
file. To refresh the results, uncomment where indicated.

# Contributing
Pull requests permitted.
```

D.2 Test Scripts

D.2.1 blockchain_test.py

```
#!/usr/bin/python3
# Python Programme to test Blockchain class
import os
import inspect
import sys
cdir = os.path.dirname(os.path.abspath(inspect.getfile(inspect.cur-
rentframe())))
parentdir = os.path.dirname(cdir)
sys.path.insert(0, parentdir)

# Setup blockchain and encryption
import json
from blockchain import Blockchain
from cryptography.fernet import Fernet
from instance.config import encryption_key
blockchain = Blockchain()
key = encryption_key

# Setup random word generation
import random
import string

candidates = [
    "Test Candidate 1",
    "Test Candidate 2",
    "Test Candidate 3",
    "Test Candidate 4",
    "Test Candidate 5",
    "Test Candidate 6",
]


# Functions sourced from: https://pynative.com/python-generate-random-
string/
def get_random_string(length):
    """Generated a random string
    of uppercase letters

    Key arguments
    length -- how long you want the string to be
    """
    # Choose from all uppercase letter
    letters = string.ascii_uppercase
    result_str = ''.join(random.choice(letters) for i in range(length))
```

```
    return result_str


def blockchain_test_block():
    """Creates a block in the existing
    chain that will randomly experience
    "interferencd" leading to the chain
    being altered.

    Key arguments
    none
    """
    previous_block = blockchain.return_previous_block()
    previous_proof = previous_block['proof']

    # Get required block variables
    proof = blockchain.proof_of_work(previous_proof)
    previous_hash = blockchain.hash(previous_block)

    pollstation = "ABC"
    secretword = get_random_string(10)
    candidate = candidates[random.randint(1, 5)]

    # Introduce random possibility of replacement block
    if random.random() < 0.01:
        candidate = candidates[0]  # Specific candidate for hacked
        previous_hash = "HACKED" + get_random_string(58)

    # Mine new block
    block = blockchain.create_block(
        proof,
        pollstation,
        secretword,
        candidate,
        previous_hash)
    block = str(json.dumps(block))


def test_blockchain(chain_length):
    """Creates a blockchain using
    the test block method which could
    be either valid or invalid and
    returns its assessment

    Key arguments
    none
    """
    i = 1
    # Create test blockchain to desired length
    while i < chain_length:
        blockchain_test_block()
        i += 1
    test_blockchain = blockchain.chain
    # Test if the chain is valid
    if blockchain.chain_valid(test_blockchain) is True:
        result = "Chain valid"
    else:
        result = "Chain not valid"
    # Return result
```

```
    final_result = [result, test_blockchain]
    # Write result to file
    with open("test/results/blockchain_test_chain.txt", "a") as
bc_test_chain:
        bc_test_chain.write("%s\n" % final_result)

# U N C O M M E N T   T O   R E F R E S H   R E S U L T S
# Run a set number of test blockchains and check their validity
# with open("test/blockchain_test_chain.txt","w") as block-
chain_test_chain:
#     i = 1
#     while i <= 200:
#         blockchain.__init__() # Initialise to refresh chain
#         test_blockchain(20) # Create test chains of 20
#         print("Test " + str(i) + " complete.")
#         i += 1


# Read positive and negative results from the file
blockchain_results = []
with open("test/results/blockchain_test_chain.txt", "r") as bc_results:
    for line in bc_results:
        result = line[:-1]  # Remove new line character
        result = result.strip('][').split(', ')
        blockchain_results.append(result)

# Create empty list to store results
results = []

# Get the count of True Positives, False Positives, True Negatives and
False Negatives
blockchain_true_positives = sum(1 for r in blockchain_results
                                if r[0] == "'Chain valid'"
                                and "HACKED" not in str(r[1:]))
blockchain_false_positives = sum(1 for r in blockchain_results
                                 if r[0] == "'Chain valid'"
                                 and "HACKED" in str(r[1:]))

blockchain_true_negatives = sum(1 for r in blockchain_results
                                if r[0] == "'Chain not valid'"
                                and "HACKED" in str(r[1:]))
blockchain_false_negatives = sum(1 for r in blockchain_results
                                 if r[0] == "'Chain not valid'"
                                 and "HACKED" not in str(r[1:]))

# Use the counts to calculate the sensitivity, specificity and accuracy
blockchain_sensitivity = blockchain_true_positives / (block-
chain_true_positives + blockchain_false_negatives) * 100
blockchain_specificity = blockchain_true_negatives / (block-
chain_false_positives + blockchain_true_negatives) * 100
blockchain_accuracy = (blockchain_true_positives + blockchain_true_nega-
tives) / (blockchain_true_positives + blockchain_false_positives +
blockchain_true_negatives + blockchain_false_negatives) * 100

# Add result to list of results
results.append(["All Results        ", blockchain_sensitivity, block-
chain_specificity, blockchain_accuracy, blockchain_true_positives,
blockchain_false_positives, blockchain_true_negatives, block-
chain_false_negatives])
```

```
# Print Results
print(results)
```

D.2.2 identification_test.py

```
#!/usr/bin/python3
# Python Programme to test Identification class
import os
import inspect
import sys
cdir = os.path.dirname(os.path.abspath(inspect.getfile(inspect.cur-
rentframe())))
parentdir = os.path.dirname(cdir)
sys.path.insert(0, parentdir)

# Setup for Identification
from identification import Identification
id = Identification()

# Add test credentials
from testdetails import myname, myaddress, mypostcode

# Create list of image paths
with open("test/test_images/filenames.txt","r") as image_filenames:
    images = image_filenames.readlines()
    images.pop(0)

    my_image_paths = []
    for i in images:
        image = "test/test_images/" + i[:-1]
        my_image_paths.append(image)


# T E X T   R E C O G N I T I O N   T E S T S

# Testing Expected Passes
def text_positive(image_paths, name, address):
    """Tests the results of the text checks
    and writes to a positive results file

    Key arguments
    image_paths -- list of image urls for images to be checked
    name -- correct name to match id
    address -- correct address to match id
    """
    print("Starting test...")
    text_positive_results = []

    # For each image in the list of files, run the text check
    for img in image_paths:
        text_result = id.check_identification_text(img, name, address)
        if (text_result[0] > 0.5 and text_result[1] > 0.5) or text_re-
sult[0] > 0.75:
            # If it passes as expected in the tool, return this result
            result = "pass"
        else:
            # else fail
```

```
            result = "fail"
        final_result = [img, result, text_result[0], text_result[1]]
        text_positive_results.append(final_result)
        with open("test/results/text_positive_results.txt","a") as p_re-
sults:
            p_results.write("%s\n" % final_result)
        print("Image " + str(len(text_positive_results)) + " complete.")

    print("Test complete.")
    return text_positive_results

# Testing Expected Failures
def text_negative(image_paths, name, address):
    """Tests the results of the text checks
    and writes to a negative results file

    Key arguments
    image_paths -- list of image urls for images to be checked
    name -- incorrect name to match id
    address -- incorrect address to match id
    """
    print("Starting test...")
    text_negative_results = []
    for img in image_paths:
        text_result = id.check_identification_text(img, name, address)
        if (text_result[0] > 0.5 and text_result[1] > 0.5) or text_re-
sult[0] > 0.75:
            result = "pass"
        else:
            result = "fail"
        final_result = [img, result, text_result[0], text_result[1]]
        text_negative_results.append(final_result)
        with open("test/results/text_negative_results.txt","a") as p_re-
sults:
            p_results.write("%s\n" % final_result)
        print("Image " + str(len(text_negative_results)) + " complete.")

    print("Test complete.")
    return text_negative_results

# U N C O M M E N T   T O   R E F R E S H   R E S U L T S
# Positive results (expecting a match)
with open("test/results/text_positive_results.txt","w") as text_posi-
tive_file:
    text_positive(my_image_paths, myname, myaddress + mypostcode)
    text_positive_file.close()
# Negative results (expecting a no match)
#with open("test/results/text_negative_results.txt","w") as text_nega-
tive_file:
    #text_negative(my_image_paths, "John Smith", myaddress.re-
place("9","8") + mypostcode)
    #text_negative_file.close()


# Read positive and negative results from the file
text_positive_results = []
text_negative_results = []
with open("test/results/text_positive_results.txt","r") as p_results:
    for line in p_results:
```

```
        result = line[:-1] # Remove new line character
        result = result.strip('][').split(', ')
        text_positive_results.append(result)

with open("test/results/text_negative_results.txt","r") as n_results:
    for line in n_results:
        result = line[:-1] # Remove new line character
        result = result.strip('][').split(', ')
        text_negative_results.append(result)

# Create empty list to store results
text_results = []

# All results
# Get the count of True Positives, False Positives, True Negatives and
False Negatives
text_true_positives = sum(1 for r in text_positive_results if r[1] ==
"'pass'")
text_false_positives = sum(1 for r in text_positive_results if r[1] ==
"'fail'")

text_true_negatives = sum(1 for r in text_negative_results if r[1] ==
"'fail'")
text_false_negatives = sum(1 for r in text_negative_results if r[1] ==
"'pass'")

# Use the counts to calculate the sensitivity, specificity and accuracy
text_sensitivity = text_true_positives / (text_true_positives +
text_false_negatives) * 100
text_specificity = text_true_negatives / (text_false_positives +
text_true_negatives) * 100
text_accuracy = (text_true_positives + text_true_negatives) /
(text_true_positives + text_false_positives + text_true_negatives +
text_false_negatives) * 100

# Add result to list of results
text_results.append(["All Results        ", text_sensitivity, text_spec-
ificity, text_accuracy, text_true_positives, text_false_positives,
text_true_negatives, text_false_negatives])

# Good Webcam Only
# Filter to only the 'good webcam' images
gw_text_positive_results = [x for x in text_positive_results if "IMG_"
in x[0]]
gw_text_negative_results = [x for x in text_negative_results if "IMG_"
in x[0]]

# Get the count of True Positives, False Positives, True Negatives and
False Negatives
gw_text_true_positives = sum(1 for r in gw_text_positive_results if r[1]
== "'pass'")
gw_text_false_positives = sum(1 for r in gw_text_positive_results if
r[1] == "'fail'")

gw_text_true_negatives = sum(1 for r in gw_text_negative_results if r[1]
== "'fail'")
gw_text_false_negatives = sum(1 for r in gw_text_negative_results if
r[1] == "'pass'")
```

```
# Use the counts to calculate the sensitivity, specificity and accuracy
gw_text_sensitivity = gw_text_true_positives / (gw_text_true_positives +
gw_text_false_negatives) * 100
gw_text_specificity = gw_text_true_negatives / (gw_text_false_positives
+ gw_text_true_negatives) * 100
gw_text_accuracy = (gw_text_true_positives + gw_text_true_negatives) /
(gw_text_true_positives + gw_text_false_positives + gw_text_true_nega-
tives + gw_text_false_negatives) * 100

# Add result to list of results
text_results.append(["Good Webcam Results", gw_text_sensitivity,
gw_text_specificity, gw_text_accuracy, gw_text_true_positives,
gw_text_false_positives, gw_text_true_negatives, gw_text_false_nega-
tives])

# Bad Webcam Only
# Filter to only the 'bad webcam' images
bw_text_positive_results = [x for x in text_positive_results if "WIN_"
in x[0]]
bw_text_negative_results = [x for x in text_negative_results if "WIN_"
in x[0]]

# Get the count of True Positives, False Positives, True Negatives and
False Negatives
bw_text_true_positives = sum(1 for r in bw_text_positive_results if r[1]
== "'pass'")
bw_text_false_positives = sum(1 for r in bw_text_positive_results if
r[1] == "'fail'")

bw_text_true_negatives = sum(1 for r in bw_text_negative_results if r[1]
== "'fail'")
bw_text_false_negatives = sum(1 for r in bw_text_negative_results if
r[1] == "'pass'")

# Use the counts to calculate the sensitivity, specificity and accuracy
bw_text_sensitivity = bw_text_true_positives / (bw_text_true_positives +
bw_text_false_negatives) * 100
bw_text_specificity = bw_text_true_negatives / (bw_text_false_positives
+ bw_text_true_negatives) * 100
bw_text_accuracy = (bw_text_true_positives + bw_text_true_negatives) /
(bw_text_true_positives + bw_text_false_positives + bw_text_true_nega-
tives + bw_text_false_negatives) * 100

# Add result to list of results
text_results.append(["Bad Webcam Results ", bw_text_sensitivity,
bw_text_specificity, bw_text_accuracy, bw_text_true_positives,
bw_text_false_positives, bw_text_true_negatives, bw_text_false_nega-
tives])

# Print text results
for r in text_results:
    print(r)


# F A C E   R E C O G N I T I O N   T E S T S

# Testing Face Positive Recognition
def face_positive(image_paths):
    """Opens the webcam and tests against
```

```
    provided images where an expected result
    is pass. Writes to positive results file.

    Key arguments
    image_paths -- list of image urls for images to be checked
    """
    print("Starting test...")
    face_positive_results = []
    for img in image_paths:
        face_result = id.check_identification_face(img)
        if face_result == "true":
            result = "pass"
        else:
            result = "fail"
        face_positive_results.append(result)
        final_result = [img, result]
        with open("test/results/face_positive_results.txt","a") as p_re-
sults:
            p_results.write("%s\n" % final_result)
        print("Image " + str(len(face_positive_results)) + " complete.")

    print("Test complete.")
    return face_positive_results

# Testing Negative Recognition
def face_negative(image_paths):
    """Opens the webcam and tests against
    provided images where an expected result
    is fail. Writes to negative results file.

    Key arguments
    image_paths -- list of image urls for images to be checked
    """
    print("Starting test...")
    face_negative_results = []
    for img in image_paths:
        face_result = id.check_identification_face(img)
        if face_result == "true":
            result = "pass"
        else:
            result = "fail"
        face_negative_results.append(result)
        final_result = [img, result]
        with open("test/results/face_negative_results.txt","a") as n_re-
sults:
            n_results.write("%s\n" % final_result)
        print("Image " + str(len(face_negative_results)) + " complete.")

    print("Test complete.")
    return face_negative_results

# U N C O M M E N T  T O  R E F R E S H  R E S U L T S
# Positive results (expecting a match)
#with open("test/face_positive_results.txt","w") as face_positive:
    #face_positive(my_image_paths)
    #face_positive.close()
# Negative results (expecting a no match)
#with open("test/face_negative_results.txt","w") as face_negative:
    #face_negative(my_image_paths)
```

```
    #face_negative.close()

# Read positive and negative results from the file
face_positive_results = []
face_negative_results = []
with open("test/results/face_positive_results.txt","r") as p_results:
    for line in p_results:
        result = line[:-1] # Remove new line character
        result = result.strip('][').split(', ')
        face_positive_results.append(result)

with open("test/results/face_negative_results.txt","r") as n_results:
    for line in n_results:
        result = line[:-1] # Remove new line character
        result = result.strip('][').split(', ')
        face_negative_results.append(result)

# Create empty list to store results
face_results = []

# All results
# Get the count of True Positives, False Positives, True Negatives and
False Negatives
face_true_positives = sum(1 for r in face_positive_results if r[1] ==
"'pass'")
face_false_positives = sum(1 for r in face_positive_results if r[1] ==
"'fail'")

face_true_negatives = sum(1 for r in face_negative_results if r[1] ==
"'fail'")
face_false_negatives = sum(1 for r in face_negative_results if r[1] ==
"'pass'")

# Use the counts to calculate the sensitivity, specificity and accuracy
face_sensitivity = face_true_positives / (face_true_positives +
face_false_negatives) * 100
face_specificity = face_true_negatives / (face_false_positives +
face_true_negatives) * 100
face_accuracy = (face_true_positives + face_true_negatives) /
(face_true_positives + face_false_positives + face_true_negatives +
face_false_negatives) * 100

# Add result to list of results
face_results.append(["All Results        ", face_sensitivity, face_spec-
ificity, face_accuracy, face_true_positives, face_false_positives,
face_true_negatives, face_false_negatives])

# Good Webcam Only
# Filter to only the 'good webcam' images
gw_face_positive_results = [x for x in face_positive_results if "IMG_"
in x[0]]
gw_face_negative_results = [x for x in face_negative_results if "IMG_"
in x[0]]

# Get the count of True Positives, False Positives, True Negatives and
False Negatives
gw_face_true_positives = sum(1 for r in gw_face_positive_results if r[1]
== "'pass'")
```

```
gw_face_false_positives = sum(1 for r in gw_face_positive_results if
r[1] == "'fail'")

gw_face_true_negatives = sum(1 for r in gw_face_negative_results if r[1]
== "'fail'")
gw_face_false_negatives = sum(1 for r in gw_face_negative_results if
r[1] == "'pass'")

# Use the counts to calculate the sensitivity, specificity and accuracy
gw_face_sensitivity = gw_face_true_positives / (gw_face_true_positives +
gw_face_false_negatives) * 100
gw_face_specificity = gw_face_true_negatives / (gw_face_false_positives
+ gw_face_true_negatives) * 100
gw_face_accuracy = (gw_face_true_positives + gw_face_true_negatives) /
(gw_face_true_positives + gw_face_false_positives + gw_face_true_nega-
tives + gw_face_false_negatives) * 100

# Add result to list of results
face_results.append(["Good Webcam Results", gw_face_sensitivity,
gw_face_specificity, gw_face_accuracy, gw_face_true_positives,
gw_face_false_positives, gw_face_true_negatives, gw_face_false_nega-
tives])

# Bad Webcam Only
# Filter to only the 'good webcam' images
bw_face_positive_results = [x for x in face_positive_results if "WIN_"
in x[0]]
bw_face_negative_results = [x for x in face_negative_results if "WIN_"
in x[0]]

# Get the count of True Positives, False Positives, True Negatives and
False Negatives
bw_face_true_positives = sum(1 for r in bw_face_positive_results if r[1]
== "'pass'")
bw_face_false_positives = sum(1 for r in bw_face_positive_results if
r[1] == "'fail'")

bw_face_true_negatives = sum(1 for r in bw_face_negative_results if r[1]
== "'fail'")
bw_face_false_negatives = sum(1 for r in bw_face_negative_results if
r[1] == "'pass'")

# Use the counts to calculate the sensitivity, specificity and accuracy
bw_face_sensitivity = bw_face_true_positives / (bw_face_true_positives +
bw_face_false_negatives) * 100
bw_face_specificity = bw_face_true_negatives / (bw_face_false_positives
+ bw_face_true_negatives) * 100
bw_face_accuracy = (bw_face_true_positives + bw_face_true_negatives) /
(bw_face_true_positives + bw_face_false_positives + bw_face_true_nega-
tives + bw_face_false_negatives) * 100

# Add result to list of results
face_results.append(["Bad Webcam Results ", bw_face_sensitivity,
bw_face_specificity, bw_face_accuracy, bw_face_true_positives,
bw_face_false_positives, bw_face_true_negatives, bw_face_false_nega-
tives])

# Print text results
for r in face_results:
```

```
    print(r)
```

D.3 stylesheet.css

```
/* Stylesheet for E-Voting Website
--------------------------------------------------------------------
*/

/* Contents
--------------------------------------------------------------------*/
/*
1.  Reset default margins, padding and borders
2.  Styling for the overall body of website
3.  Styling for the header portion of website
4.  Styling for the Navigation Bar of website
5.  Place the main and right hand side content next to each other
6.  Styling for main content of the website
7.  Styling for any right hand side content of the website
8.  Styling for the footer of website
9.  FAQ Styling
10. Styling for webcam image displays
*/

/* 1. Reset default margins, padding and borders
--------------------------------------------------------------------
*/
* {
    margin: 0;
    padding: 0;
    box-sizing: border-box;
  }

  /* 2. Styling for the overall body of website
  --------------------------------------------------------------------
*/
  body {
    background-color: #F3F2F1;
    font-family: Arial, sans-serif;  /* Set standard font for entire
website */
    font-size: calc(15px + 0.390625vw);
  }



  /* 3. Styling for the header portion of website
  --------------------------------------------------------------------
*/
  .header {
    display: flex;
    padding: 3%;
    background: #1D70B8;
    text-align: center;
    margin-bottom: 5%;
  }

  .header h1 {
    color: white;
```

```
    font-size: 5vw;
    font-weight:lighter;
    width: 100%;
    float: left;
    margin-top: 1%;
  }
  .header img {
    width: 8%;
    height: 8%;
    float: left;
  }

  /* 3. Middle Section of the website
  ----------------------------------------------------------------------
*/
  .middle {
    margin: auto;
    padding: 2%;
    border-width: 5%;
    border-radius: 25px;
    width: 80%;
    text-align: center
  }

  .middle h1 {
    color: black;
    font-size: calc(30px + 0.390625vw);

  }
  .middle p {
    padding: 4%;
  }

  .middle #candidates {
    padding: 2.5%;
    text-align: left;
    margin-left: 1%;
    font-size: 1.25vw
  }

  .middle img {
    width: 4vw;
    height: 4vw;
    padding: 1%
  }

  .middle select {
    padding: 1%
  }

     /* 2. Button syling
  ----------------------------------------------------------------------
*/
  .button {
    margin: auto;
    margin-top: 2%;
    border-radius: 11px;
    font-family: Arial;
    color: #ffffff;
```

```
    padding: 0.5vw 2vw 0.5vw 2vw;
    text-decoration: none;
    text-align: center;
  }
  .button a {
    background: #000000;
    text-decoration: none;
  }
  .button a:hover {
    background: #1d70b8;
    text-decoration: none;
  }

     /* 2. HTML Input Styling
  ------------------------------------------------------------------------
*/

  input[type=submit] {
    margin: auto;
    margin-top: 1%;
    margin-bottom: 1%;
    border-radius: 11px;
    font-family: Arial;
    color: #ffffff;
    padding: 0.5vw 2vw 0.5vw 2vw;
    text-decoration: none;
    text-align: center;
    background: #000000;
    text-decoration: none;
    font-size: calc(15px + 0.390625vw);
    display: block;
  }

  input[type=submit]:hover {
    background: #1d70b8;
    text-decoration: none;
  }

  input[type=text] {
    font-size: calc(15px + 0.390625vw);
  }

  /* Source: https://www.sliderrevolution.com/resources/styling-radio-
buttons/ */
  .custom-radios div {
    display: inline-block;
    text-align: left;
    width: calc(500px + 0.390625vw);
    margin: auto;
    padding: 0.5%;
    font-size: calc(10px + 0.390625vw);
    max-width: 95%;
  }

  .custom-radios input[type="radio"] {
    display: none;
  }
  .custom-radios input[type="radio"] + label {
    color: black;
```

```
  font-family: Arial, sans-serif;

}
.custom-radios input[type="radio"] + label span {
  display: inline-block;
  box-sizing: border-box;
  appearance: none;
  width: calc(40px + 0.390625vw);
  height: calc(40px + 0.390625vw);
  vertical-align: middle;
  /* Make cursor a pencil when hovering over */
  cursor:  url('pencil_cursor.ico'), auto;
  outline: 2px solid black;
  background: white;
  background-repeat: no-repeat;
  background-position: center;
  margin-right: 1.5%;
}
.custom-radios img {
  opacity: 0;
  transition: all 0.3s ease;
  width: calc(40px + 0.390625vw);
  height: calc(40px + 0.390625vw);
}
.custom-radios input[type="radio"] + label span img {
  opacity: 0;
  transition: all 0.3s ease;
}
.custom-radios input[type="radio"]:checked + label span img {
  opacity: 1;
}

/* 8. Styling for the footer of website
-------------------------------------------------- */
.page-container {
  position: relative;
  min-height: 100vh;
}

.content-wrap {
  padding-bottom: 3rem;    /* Footer height */
}

.footer {
  position: absolute;
  bottom: 0;
  left: 0;
  width: 100%;
  height: 3rem;            /* Footer height */
  background-color: #1D70B8;
  text-align: center;
}

.footer p {
  padding-top: 0.5rem;
  padding-bottom: 1rem;
  color: white;
  font-size: 0.7rem;
}
```

```
  /* 9. FAQ Styling
  ----------------------------------------------- */
  div#faqs p{
    display:none;
  }

  div#faqs p.faq1:target {
    display:block;
  }
  div#faqs p.faq2:target {
    display:block;
  }
  div#faqs p.faq3:target {
    display:block;
  }
  div#faqs p.faq4:target {
    display:block;
  }
  div#faqs h3 {
    padding: 1%;
    font-weight: bold;
  }
  div#faqs a:visited {
    color: black;
  }
  div#faqs a:hover {
    color: #1d70b8;
  }

  /* 10. Styling for webcam image displays
  ----------------------------------------------- */
  #video-container {
    width: 100%;
    max-width: 640px;
    margin: auto;
    display: block;
}

#captured-image {
    display: none;
    width: 100%;
    max-width: 640px;
    height: auto;
    margin: auto;
}
```

D.4 HTML Templates

D.4.1 0_index.html

```
<!DOCTYPE html>
<html lang="en">
<head>
    <!-- Basic Page Needs
```

```
         ------------------------------------------------- -->
         <meta charset="utf-8">
         <title>Internet E-Voting Tool</title>
         <meta name="description" content="Welcome page for the e-voting
system">
         <meta name="author" content="Cheylea Hopkinson">
         <!-- CSS
            ------------------------------------------------- -->
         <link rel= "stylesheet" type= "text/css" href=
"{{ url_for('static',filename='css/stylesheet.css') }}">
         <!-- Favicon
            ------------------------------------------------- -->
         <link rel="icon" type="image/png" href="{{ url_for('static',
filename='images/ballot_box.png') }}">
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-
scale=1.0">
    <title>Home</title>
</head>
<body>
    <div class="page-container">
      <div class="content-wrap">

        <!-- Page Header -->
        <div class="header">
          <img src=
          "{{url_for('static',filename='images/ballot_box_large.png')}}"
alt=
          "Ballot box with Ballot" style="float: left;" />

            <h1>Electronic Voting Tool</h1>

          <img src=
          "{{url_for('static',filename='images/ballot_box_large.png')}}"
alt=
          "Ballot box with Ballot" style="float: right;" />
        </div>

        {% block content %}

        <div class="middle">
          <h1>Welcome</h1>

          <p>This website will take you through voting in this Election.
You will need your name and poll number as found on your poll card.
          <br>
          <br>
          You can exit the tool at any time by closing the tab/window.
          <br>
          Please note, if you do not complete the full voting process
your vote will not be counted.</p>
          <div class="middle-button">
            <div class="button">
              <a href="/faqs" class="button">Continue</a>
            </div>
          </div>
        </div>

        {% endblock %}
```

```
        <!-- Page Footer -->
        <div class="footer">
          <p>This website was created for educational purposes. All
rights reserved &#169; Cheylea Hopkinson
          2023.</p>
        </div>
      </div>
    </div>
  </body>
  </html>
```

D.4.2 1_indextest.html

```
<!DOCTYPE html>
<html lang="en">
<head>
    <!-- Basic Page Needs
         ---------------------------------------------------- -->
         <meta charset="utf-8">
         <title>Cheylea Hopkinson</title>
         <meta name="description" content="Welcome page for the e-voting
system">
         <meta name="author" content="Cheylea Hopkinson">
         <!-- CSS
            ---------------------------------------------------- -->
         <link rel= "stylesheet" type= "text/css" href=
"{{ url_for('static',filename='css/stylesheet.css') }}">
         <!-- Favicon
            ---------------------------------------------------- -->
         <link rel="icon" type="image/png" href="{{ url_for('static',
filename='images/ballot_box.png') }}">
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-
scale=1.0">
    <title>Home</title>
</head>
<body>
    <div class="page-container">
      <div class="content-wrap">

        <!-- Page Header -->
        <div class="header">
          <img src=
          "{{url_for('static',filename='images/ballot_box_large.png')}}"
alt=
          "Ballot box with Ballot" style="float: left;" />

            <h1>Electronic Voting Tool</h1>

          <img src=
          "{{url_for('static',filename='images/ballot_box_large.png')}}"
alt=
          "Ballot box with Ballot" style="float: right;" />
        </div>

        {% block content %}
```

```
        <div class="middle">
          <h1>Welcome</h1>

          <p>You are invited to take part in this research study involv-
ing the review of
          a prototype electronic voting tool. This will involve follow-
ing through this application,
          simulating a vote of your choice, and filling out a survey
questionnaire.
          <br>
          <br>
          You can exit the tool at any time by closing the tab/window.
          <br>
          Please note, if you do not complete the test sequence, we will
be unable to use your survey answers.</p>
          <div class="middle-button">
            <div class="button">
              <a href="/faqs" class="button">Continue to Test</a>
            </div>
          </div>
        </div>

        {% endblock %}

        <!-- Page Footer -->
        <div class="footer">
          <p>This website was created for educational purposes. All
rights reserved &#169; Cheylea Hopkinson
          2023.</p>
        </div>
      </div>
    </div>
  </body>
  </html>
```

D.4.3 2_faqs.html

```
{% extends '0_index.html' %}

{% block content %}
<div class="middle">
    <h1>Frequently Asked Questions</h1>
    <br>
    <p style="padding: 0.5%;">
        Carefully read through the answers below by clicking each ques-
tion.
    </p>
    <br>
    <div id='faqs'>
        <h3><a href="#faq1" class="nav-tab tab1">How does the voting
work?</a></h3>
        <p id='faq1' class='faq1'>The voting tool will first check if
you are able to vote and perform an identity check*.
            You can then select a candidate to vote for. When voting,
you will be asked to provide a secret word. Once you cast
            your vote, a technology called 'blockchain' is used to rec-
ord your vote such that it can't be changed. For five minutes
```

```
            after voting, you will be able to view the candidate you
voted for. This is a way of verifying the correct
            vote has been cast by using your secret word.
            <br>
            <br>
            *This test version will <b>NOT</b> perform any checks, so we
will not collect any of your personal details.</p>
    </div>
    <div id='faqs'>
        <h3><a href="#faq2" class="nav-tab nav-tab-active tab2">What is
blockchain?</a></h3>
          <p id='faq2' class='faq2'>Blockchain is a way of storing data.
Pieces of data are stored in 'blocks'.
            Once stored, they cannot be changed. Each block contains
data that can connect it to the previous block.
            This means data is stored as a chain of block data that only
has one order. Votes are collected without
            your personal data. Instead, a secret word of your choosing
is used to maintain the anonymity of your vote.
            When storing the blocks, these are published in multiple
places. This means people will be able to see and
            view the data stored when your vote is collected. </p>
    </div>
    <div id='faqs'>
        <h3><a href="#faq3" class="nav-tab tab3">How can I know my vote
will be counted correctly?</a></h3>
          <p id='faq3' class='faq3'>Blockchain data cannot be changed.
Once your vote is stored, that is the
            vote that will be counted. This tool allows you to view your
unchangeable vote after it is stored. This is
            so you can verify the vote is the candidate you selected.
This is only available up to five minutes after
            you cast your vote and will require you to remember your se-
cret word.</p>
    </div>

    <div id='faqs'>
        <h3><a href="#faq4" class="nav-tab tab4">What can I use for my
secret word?</a></h3>
          <p id='faq4' class='faq4'>You can use a word or phrase up to
15 letters. However, you can't use any names of other
            voters or addresses. You also can't use a word that has al-
ready been used by another voter at your polling station.
            Try to choose something easy to remember.
            <br>
            <br>
            <b>Please be aware, if you forget your secret word you will
not be able to verify your vote.</b></p>
        </div>

        <div class="button">
            <a href="/checkeligibility" class="button">Continue</a>
        </div>
</div>

{% endblock %}
```

D.4.4 3_checkeligibility.html

```
{% extends '0_index.html' %}

{% block content %}
<div class="middle">
    <h1>Check if you can vote</h1>
    <p>Please provide your name and poll number as it appears on your
poll card.
        <br>
    </p>
    <form action="{{ url_for("verifyeligibility")}}" method="post">
        <label for="tester">For the purposes of this demonstration,
please select from the below test credentials:</label>
        <br>
        <br>
        <select id="tester" name="tester">
        <!-- Goes through each test name in the database to display in a
list -->
        {% for voter in test_voters %}
        <option value='{{voter.pollstation}}{{voter.poll-
number}}'>{{voter[1]}}{{voter[2]}} - {{voter[3]}}</option>
        {% endfor %}
    </form>
</div>
    <div class="button">
        <input type="submit" value="Continue">
    </div>
</div>
{% endblock %}
```

D.4.5 4_checkeligibilitytest.html

```
{% extends '0_index.html' %}

{% block content %}
<div class="middle">
    <h1>Check if you can vote</h1>
    <p>When voting in person, you are asked at the polling booth to pro-
vide your poll number or name and first line of your address to vote
with.
        In a real version of this tool, you would enter either your poll
number or name and address to check you are able to vote.
        <br>
        <br>
        For the purposes of this survey, we have provided some test
voter details to choose from.
        <br>
    </p>
    <form action="{{ url_for("verifyeligibility")}}" method="post">
        <label for="tester">Please select any of the below test creden-
tials:</label>
        <br>
        <br>
        <select id="tester" name="tester">
        <!-- Goes through each test name in the database to display in a
list -->
        {% for voter in test_voters %}
```

```
        <option value='{{voter.pollstation}}{{voter.poll-
number}}'>{{voter[1]}}{{voter[2]}} - {{voter[3]}}</option>
        {% endfor %}
    </form>
</div>
    <div class="button">
        <input type="submit" value="Continue">
    </div>
</div>
{% endblock %}
```

D.4.6 5_verifyid.html

```
{% extends '0_index.html' %}

{% block content %}
<div class="middle">
    <h1>Identification Check</h1>
    <p>You will now be asked to take a photo of your Driving Licence or
Provisional Licence.
    <br>
    Once completed, your webcam will turn on and your face will be com-
pared to your license, alongside your name and address.
    Please ensure your face is facing the webcam ready to be checked
upon submission of the photo of your id.
    <br>
    </p>
</div>
<div class="middle-button">
    <div class="button">
        <a href="/idphoto/{{ pollnumber }}" class="button">Check Iden-
tity</a>
    </div>
</div>
{% endblock %}
```

D.4.7 5_verifyidtest.html

```
{% extends '0_index.html' %}

{% block content %}
<div class="middle">
    <h1>Identification Check</h1>
    <p>At this stage in the process, you would be asked to provide your
photo identification and take a live photo of yourself.
    <br>
    For the purposes of this prototype, you will not need to provide ei-
ther of these.
    <br>
    <b>{{ name }}</b> will automatically pass the identification check.
    </p>
</div>
<div class="middle-button">
    <div class="button">
        <a href="/enterword/{{ pollnumber }}" class="button">Check Iden-
tity</a>
    </div>
```

```
</div>
{% endblock %}
```

D.4.8 5a_idphoto.html

```
{% extends '0_index.html' %}

{% block content %}
<div class="middle">
    <h1>Identification Check</h1>
    <p> Please hold your driving licence or provisional driving licence
up to the camera and ensure a clean image is taken of it.
    <br>
    Click the button to take the image
    <br>
    </p>

    <!-- Video container for the webcam -->
    <div id="video-container">
        <video id="video" width="640px" autoplay></video>
        <img id="captured-image" alt="Captured Image">
    </div>

    <!-- Buttons to capture, try again and check identity -->
    <div class="button">
        <div id="capture-buttons">
            <a id="capture-button" onclick="captureImage()" class="but-
ton">Capture</button>
            <a id="try-again-button" onclick="tryAgain()" style="dis-
play: none;" class="button">Try Again</button>
            <a id="checkidentity-button" onclick="checkIdentity()"
style="display: none;" class="button">Check Identity</button>
        </div>
    </div>
</div>


<script>
        // Access the webcam
        let video = document.getElementById('video');
        let canvas = document.getElementById('canvas');
        let capturedImage = document.getElementById('captured-image');
        let captureButtons = document.getElementById('capture-buttons');
        let imageCapture;

        // Capture images from the webcam
        navigator.mediaDevices.getUserMedia({ video: true })
            .then(function (stream) {
                video.srcObject = stream;
                imageCapture = new ImageCapture(stream.getVide-
oTracks()[0]);
            })
            // Error if cannot access the webcam
            .catch(function (err) {
                console.error('Error accessing webcam: ', err);
            });

            function captureImage() {
```

```
            // Take photo and display on screen
            imageCapture.grabFrame().then(imageBitmap => {
                const canvas = document.createElement('canvas');
                canvas.width = imageBitmap.width;
                canvas.height = imageBitmap.height;
                const context = canvas.getContext('2d');
                context.drawImage(imageBitmap, 0, 0, canvas.width, can-
vas.height);
                capturedImage.src = canvas.toDataURL('image/png');
                capturedImage.style.display = 'block';
                captureButtons.style.display = 'block';

                // Stop the webcam and hide it from the screen
                const tracks = video.srcObject.getTracks();
                tracks.forEach(track => track.stop());
                video.style.display = 'none';

                // Hide capture button
                document.getElementById('capture-button').style.display
= 'none';
                // Display buttons to try taking photo again or continu-
ing
                document.getElementById('try-again-button').style.dis-
play = 'block';
                document.getElementById('checkidentity-but-
ton').style.display = 'block';
            });

        }

        // Reload the page to try again
        function tryAgain() {
            location.reload();
        }

        // Continue on to identity check
        function checkIdentity() {
            // Extract poll number
            // Extract the parameter value from the URL
            let paths = window.location.pathname.split('/');
            let pollnumber = paths[paths.length - 1];

            // Store the image
            let imagedata = capturedImage.src.split(',')[1];
            fetch('/storephoto/' + pollnumber, {
                method: 'POST',
                headers: {
                    'Content-Type': 'application/x-www-form-urlencoded',
                },
                body: `imagedata=${encodeURIComponent(imagedata)}&poll-
number=${pollnumber}`,
            })
            // Read response from page
            .then(response => response.json())
            .then(data => {
                console.log('Response from server:', data); // Log re-
sponse for debugging
                if (data.status === 'success') {
                    console.log('success')
```

```
                    // If passed, redirect to the passedidcheck page
                    window.location.href = `/passedidcheck/${poll-
number}`;
                } else {
                    console.log('fail')
                    // If failed, redirect to the failedidcheck page
                    window.location.href = `/failedidcheck/${poll-
number}}`;
                }
            })

            // Hide both the Try again and continue buttons
            document.getElementById('try-again-button').style.display =
'block';
            document.getElementById('checkidentity-button').style.dis-
play = 'block';

        }
    </script>


{% endblock %}
```

D.4.9 5a_idphoto_pass.html

```
{% extends '0_index.html' %}

{% block content %}
<div class="middle">
    <h1>Identification Check Passed!</h1>
    <p>
        Congratulations you have passed your id check and may move on to
voting.
    </p>
</div>
<div class="middle-button">
    <div class="button">
        <a href="/enterword/{{ pollnumber }}" class="button">Continue to
Vote</a>
    </div>
</div>
{% endblock %}
```

D.4.10 5a_idphoto_fail.html

```
{% extends '0_index.html' %}

{% block content %}
<div class="middle">
    <h1>Identification Check Failed</h1>
    <p>
        Unforunately there has been an issue verifying you identity.
Please contact your local authority for help.
    </p>
</div>
<div class="middle-button">
    <div class="button">
```

```
        <a href="/" class="button">Back to Home</a>
    </div>
</div>
{% endblock %}
```

D.4.11 6_enterword.html

```
{% extends '0_index.html' %}

{% block content %}
<div class="middle">
    <h1>Secret Word</h1>

    <!-- Return the word to the form for checking -->
    <form action="{{ url_for('enterwordcheck', pollnumber=poll-
number) }}", method="post">
    <p>Your secret word will be used to verify your vote. Remember: you
can use a word or phrase up to 15 letters.
        However, you can't use any names of other voters or addresses.
You also can't use a word that has already been used by another
        voter at your polling station. Try to choose something easy to
remember.
        <br>
        <br>
        <b>Please be aware, if you forget your secret word you will not
be able to verify your vote.</p>
    <p style = "color: red; font-weight: bold; padding: 2%">{{ er-
rormessage }}</p>
        <label for="sword">Enter your secret word:</label><br>
        <br>
        <input type="text" id="sword" name="sword" style="text-trans-
form:uppercase" maxlength="15"><br>
    </div>
        <div class="button">
            <input type="submit" value="Click here to submit word">
        </div>
    </form>


{% endblock %}
```

D.4.12 7_vote.html

```
{% extends '0_index.html' %}

{% block content %}
<div class="middle">
    <h1>Vote</h1>
    <p style = "padding: 1%">Please choose ONE of the candidates below
to vote for.</p>
    <!-- Submit the results to the form -->
    <form action="{{ url_for('submitvote', pollnumber=pollnumber,
secretword = secretword) }}", method="post">
    <p style = "padding: 1%">Choose your candidate:</p><br>
    <div class="custom-radios">
        <!-- List each available candidate in the window -->
        {% for candidates in candidates %}
```

```
        <div>
        <input type="radio" id="{{candidates.candidatename}}" name="can-
didates" value="{{candidates.candidatename}}">
        <label for="{{candidates.candidatename}}">
          <span>
            <img src="{{url_for('static',filename='images/cross.svg')}}"
alt="Checked Icon" />
          </span>
          </label>
          {{candidates[1]}} - {{candidates[2]}}
        </div>
        {% endfor %}
        <!-- Render the check buttons and non-vote option -->
        <p style = "padding: 1.5%"></p>
        <div>
        <input type="radio" id="I would like my vote to register as a
non-vote" name="candidates" value="{{candidates.candidatename}}">
        <label for="I would like my vote to register as a non-vote">
          <span>
            <!-- Marked with a cross when checkbox is selected-->
            <img src="{{url_for('static',filename='images/cross.svg')}}"
alt="Checked Icon" />
          </span>
          </label>
          I would like my vote to register as a non-vote
        </div>
    </div>
    <br>
    <div class="middle-button">
        <div class="button">
            <!-- Alter user to confirm their vote-->
            <input type="submit" onclick="return confirm('Check your se-
lection. Do you still wish to continue?')" value="Click here to submit
vote">
        </div>

    </div>
    </form>


{% endblock %}
```

D.4.13 8_complete.html

```
{% extends '0_index.html' %}

{% block content %}
<div class="middle">
    <h1>Complete</h1>
    <p>Your vote has been cast!
    </p>
</div>
<div class="middle-button">
    <div class="button">
        <a href="/verify" class="button">Click here to continue to check
your vote</a>
    </div>
</div>
```

```
{% endblock %}
```

D.4.14 9_verify.html

```
{% extends '0_index.html' %}

{% block content %}
<div class="middle">
    <h1>Verify your vote</h1>
    <!-- Receipt input for secret word for vote verification-->
    <form action="{{ url_for('fetchvote', pollstation=pollstation,
secretword = secretword) }}", method="post">
    <p>You are able to view your vote by entering your secret word for
five minutes after submitting. </p>
    <p style = "color: red; font-weight: bold; padding: 2%">{{ er-
rormessage }}</p>
        <label for="sword">Enter your secret word:</label><br>
        <br>
        <input type="text" id="sword" name="sword" style="text-trans-
form:uppercase" maxlength="15"><br>

        <label for="sword">Enter your poll station: *</label><br>
        <br>
        <input type="text" id="pollstation" name="pollstation"
style="text-transform:uppercase" maxlength="15" value="ABC"><br>

        <p>* all test credentials have polling station "ABC"</p>
    </div>
    <div class="middle-button">
        <div class="button">
            <input type="submit" value="Click here to verify vote">
        </div>
    </div>
    </form>
{% endblock %}
```

D.4.15 10_seevote.html

```
{% extends '0_index.html' %}

{% block content %}
<div class="middle">
    <h1>Verify Identification</h1>
    <p style = "color: red; font-weight: bold; padding: 2%">{{ er-
rormessage }}</p>
    <p style = "padding: 2%">{{ candidate }}</p>
    <div class="button">
        <a href="/verify" class="button">Try Again</a>
    </div>
    <p style = "padding: 2%">You may now close the window.</p>
</div>
{% endblock %}
```

D.4.16 10_seevotetest.html

```
{% extends '0_index.html' %}
```

```
{% block content %}
<div class="middle">
    <h1>Verify Identification</h1>
    <p style = "color: red; font-weight: bold; padding: 2%">{{ er-
rormessage }}</p>
    <p style = "padding: 2%">{{ candidate }}</p>
    <div class="button">
        <a href="/verify" class="button">Try Again</a>
    </div>
    <p>Thank you for taking part in this survey. To prove you have
tested the tool, copy the word below and paste it into the survey ques-
tion:
        <i>"What word was shown on screen at the end of the
test?"</i></p>
    <h1 style = "color: rgb(14, 86, 137); font-weight: bold; padding:
0%;">CANDIDATE</h1>
    <br>
    <p style = "padding: 2%">You may now close the window.</p>
</div>
{% endblock %}
```

D.4.17 error.html

```
{% extends '0_index.html' %}

{% block content %}
<div class="middle">
    <h1>Error</h1>
    <p>Something went wrong! Please contact you local authority for as-
sistance.</p>
</div>

{% endblock %}
```

Appendix E. SURVEY

E.1 Questions

Electronic Voting Tool Survey

Research project: Exploring Solutions to Internet Voting in Government Elections in the UK

Name of researcher(s): Cheylea Hopkinson

Section 1

Participant Information

Click here to read through the information sheet for this survey:

https://drive.google.com/file/d/1aCmXZ7vFDU9nj96o5XYjqodi5LEj9eXB/view?usp=sharing

1. Please select each box to confirm your consent to take part in this survey. Required to answer. Multiple choice.

Please select 8 options.

1. I confirm that I have read and have understood the information sheet dated 26/06/2023 for the above study, or it has been read to me. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily.

2. I understand that taking part in the study involves reviewing an electronic voting tool and answering questions about it.

3. I understand that my participation is voluntary and that I am free to stop taking part and can withdraw from the study at any time without giving any reason and without my rights being affected. In addition, I understand that I am free to decline to answer any particular question or questions.

4. I understand that my responses will be kept strictly confidential. I give permission for members of the research team to have access to my fully anonymised responses. I understand that my name will not be linked with the research materials, and I will not be identified or identifiable in the report or reports that result from the research.

5. I understand that I can ask for access to the information I provide, and I can request the destruction of that information if I wish at any time prior to the survey being complete. I understand that following survey completion I will no longer be able to request access to or withdrawal of the information I provide.

6. I understand that the information I provide will be held securely and in line with data protection requirements at the University of Liverpool until it is fully anonymised and then later destroyed.

7. I understand that signed consent forms and survey answers will be retained in the University network drive until the written findings are complete.

8. I agree to take part in the above study.

Section 2

Screening

This section will check if you are eligible to take part in this survey.

2. Are you over the age of 18? Required to answer. Single choice.

- Yes
- No

3. Have you previously voted in an election in the UK (local or general)? Required to answer. Single choice.

- Yes
- No

Section 3

Thank you for considering taking part in this survey

Unfortunately you do not complete the requirements for completing this survey.

Section 4

Background Questions

This section is used to collect background information related to this survey.

4. How do you normally vote? Required to answer. Single choice.

- In person
- By post
- By proxy

5. What is your age bracket? Required to answer. Single choice.

- 18-24
- 25-39
- 40-59
- 60-79
- Over 80

6. Are you currently eligible to vote in the UK? Required to answer. Single choice.

- Yes
- No
- I don't know

7. How many times have you voted in a UK local or general election? Required to answer. Single choice.

- Less than 5 times
- 5-10 times
- 10-15 times
- Over 15 times

8. Have you ever heard of electronic voting? Required to answer. Single choice.

- Yes
- No

9. Would you be more likely to vote if electronic voting was an option? Required to answer. Single choice.

- Yes
- No
- Maybe
- I don't know

10. Would you ever consider voting electronically as opposed to voting by paper? Required to answer. Single choice.

- Yes
- No

11. Do you agree or disagree with the following statement:

    Electronic voting is a good thing that should be used in the UK. Required to answer. Single choice.

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly disagree

12. If electronic voting was introduced, what would worry you? (Tick all that apply) Required to answer. Multiple choice.

- It feels like too high of a risk
- I don’t understand how electronic voting works
- I don’t understand how electronic voting could be safe
- Voting in person is an important experience to have
- I prefer paper voting
- More research is required before we can do it safely
- I want my identity to be safe and/or stay anonymous online
- I cannot trust it to count my vote correctly
- I am worried I would do it wrong
- I don't want my data to be misused
- I have no worries or concerns

13. Do you have any other thoughts on electronic voting? Multi Line Text.

    Enter your answer

14. Have you ever heard of blockchain? Required to answer. Single choice.

- Yes
- No

15. Could you easily describe how blockchain works? Required to answer. Single choice.

- Yes
- No

16. Do you know how blockchain could link to electronic voting? Required to answer. Single choice.

- Yes
- No

17. Do you have any other thoughts on blockchain? Multi Line Text.

    Enter your answer

18. Do you agree or disagree with the following statement:

    The new requirement to show photographic ID at polling stations in the UK to vote is a good thing. Required to answer. Single choice.

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly disagree

Section 5

Electronic Voting Tool Test

Electronic voting is an alternative method to voting through paper ballots. This research project has put together a prototype for a type of electronic voting tool. Please follow the link here to access the tool and complete a simulated electronic vote. Read the instructions and information carefully as you go.

https://www.selfverificationelectronicvotingtool.co.uk/

Section 6

Screening Questions

This question is to check you have completed the electronic voting tool test. If the answer does not match, the survey answers will be excluded.

19. What word was shown on screen at the end of the test? Required to answer. Single line text.

    Enter your answer

Section 7

Reviewing the tool

This section is to gather your thoughts on the electronic voting tool.

20. How easy what it to understand how to use the tool? Required to answer. Single choice.

- Extremely easy
- Somewhat easy
- Neutral
- Somewhat not easy
- Extremely not easy

21. How clear was the information provided on how the tool works? Required to answer. Single choice.

- Extremely clear
- Somewhat clear
- Neutral
- Somewhat not clear
- Extremely not clear

22. Do you agree or disagree with the following statement:

    I can trust the electronic voting tool to count my vote correctly. Required to answer. Single choice.

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly Disagree

23. Do you agree or disagree with the following statement:

    I would be comfortable providing a photo or video of myself with a photo of my ID card to confirm my identification when voting. Required to answer. Single choice.

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly disagree

24. Are there any other things you liked about the tool? Multi Line Text.

    Enter your answer

25. Are there any other things you were concerned about, didn't like or thought could be improved about the tool? Multi Line Text.

    Enter your answer

Section 8

Review Questions

This section is to determine if your views around electronic voting may be different.

26. Having tested the tool, would you be more likely to consider electronic voting in the future? Required to answer. Single choice.

- Yes
- No
- Maybe
- I don't know

27. Do you agree or disagree with the following statement:

    Electronic voting is a good thing that should be used in the UK. Required to answer. Single choice.

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly disagree

28. If electronic voting was introduced in a similar way to the tested tool, what would still worry you? (Tick all that apply) Required to answer. Multiple choice.

- It feels like too high of a risk
- I don’t understand how electronic voting works
- I don’t understand how electronic voting could be safe
- Voting in person is an important experience to have
- I prefer paper voting
- More research is required before we can do it safely
- I want my identity to be safe and/or stay anonymous online
- I cannot trust it to count my vote correctly
- I am worried I would do it wrong
- I don't want my data to be misused
- I have no worries or concerns

29. Do you have a stronger understanding of blockchain and how it works? Required to answer. Single choice.

- Yes
- No
- Maybe
- I don't know

30. What is the one main advantage of electronic voting for you? Required to answer. Multi Line Text.

    Enter your answer

31. What is the one main drawback of electronic voting for you? Required to answer. Multi Line Text.

    Enter your answer

32. Please provide any other thoughts below. Multi Line Text.

    Enter your answer

E.2 Information Sheet

Survey Participant Information Sheet

Study: Exploring Solutions to Internet Voting in Government Elections in the UK

Version 1.1: 26/06/2023

You have been invited to take part in a research study involving the review of an IT application and filling out a survey questionnaire. Before participating, please carefully read the following information about the study that will detail its purpose and aims. Reading through all the information is important so that you understand what is involved with participating in the research and allow you to decide if you would like to take part. If anything is unclear, or you have any further questions, please contact the researcher, Cheylea Hopkinson, at C.Z.L.Hopkinson@liverpool.ac.uk. There is no obligation to take part in this study.

1. What is the purpose of the study?

This study is being conducted to explore a potential electronic voting method and whether a voter may be content that a vote they cast electronically would be correctly counted. In the UK, we still use paper voting, which has a few disadvantages such as cost and inconvenience. However, it is a familiar system that is straightforward and easy for most voters to understand. Finding an electronic method that is secure and can provide two-way transparency between the voter and governing body is more difficult, and this study aims to explore if a particular method could solve this problem.

2. Why have I been chosen to take part?

Any participant that is eligible to vote in the UK can take part in this study to gather feedback from individuals this directly affects.

3. Do I have to take part?

There is no obligation to complete the study. Before submission, no data will be kept and exiting the survey will be taken as a withdrawal and no data will be collected. If you have already submitted your survey data, you will have one month after the completion date to request data withdrawal. All data will be anonymised once collected, and no data will be kept once the research is complete.

4. What will happen if I take part?

The survey will start with a series of questions to gain your understanding and position on electronic voting before beginning. Once complete, a link will be shared that will take you to a testing version of the electronic voting tool. Once you have completed reviewing the tool, you will be asked a series of questions to get your feedback on the tool.

The research is being conducted by master's student, Cheylea Hopkinson, who is completing this study for her master's dissertation project. The full survey only needs to be completed once and will take approximately 30 minutes in total. Participants are urged to answer as honestly as they can to ensure accuracy of the results.

5. How will my data be used?

The University processes personal data as part of its research and teaching activities in accordance with the lawful basis of 'public task', and in accordance with the University's purpose of "advancing education, learning and research for the public benefit".
Under UK data protection legislation, the University acts as the Data Controller for personal data collected as part of the University's research. The Principal Investigator acts as the Data Processor for this study, and any queries relating to the handling of your personal data can be sent to Cheylea Hopkinson at C.Z.L.Hopkinson@liverpool.ac.uk.
Further information on how your data will be used can be found in the table below.

How will my data be collected?	Data is collected via an online survey form.
How will my data be stored?	Data is encrypted online and then downloaded and stored securely on the university network drive.
How long will my data be stored for?	Data will be destroyed upon completion of the dissertation in January 2024.
What measures are in place to protect the security and confidentiality of my data?	No identifiable information will be collected.
Will my data be anonymised?	Data will anonymised upon collection such that no singular person can be identified.
How will my data be used?	The data will collect feedback about the electronic voting method and answers will be analysed in the written findings.
Who will have access to my data?	The Principal Investigator and Dissertation Advisor
Will my data be archived for use in other research projects in the future?	No
How will my data be destroyed?	As the data is digital, all copies will be fully deleted.

6. Are there any risks in taking part?

The survey questions are non-invasive and do not collect any identifiable information to protect your privacy. If for any reason when taking part in the survey you feel uncomfortable or no longer want to continue, you can stop the survey and no data will be collected.

7. Are there any benefits in taking part?

There is no intended benefit beyond the opportunity to contribute to the body of academic knowledge around this topic.

8. What will happen to the results of the study?

The study will be summarised within the dissertation project. The survey results will be analysed by looking at proportional answers to questions and comparing across different groups like age groups and voting experience. If you are interested in seeing the results of the study, please contact Cheylea Hopkinson at C.Z.L.Hopkinson@liverpool.ac.uk and this can be provided once the written findings are complete. Please note that no participant will be identifiable in the written findings.

9. What will happen if I want to stop taking part?

If for any reason you want to stop taking part, you can stop the survey at any time and any data already collected from you will also be fully deleted and not stored. However, upon submission, data will be anonymized and data that has already been anonymized cannot be destroyed.

10. What if I am unhappy or if there is a problem?

If you are unhappy, or if there is a problem, please feel free to let us know by contacting Cheylea Hopkinson at C.Z.L.Hopkinson@liverpool.ac.uk and we will try to help. If you remain unhappy or have a complaint which you feel you cannot come to us with then you should contact the Research Ethics and Integrity Office at ethics@liv.ac.uk. When contacting the Research Ethics and Integrity Office, please provide details of the name or description of the study (so that it can be identified), the researcher(s) involved, and the details of the complaint you wish to make.

The University strives to maintain the highest standards of rigour in the processing of your data. However, if you have any concerns about the way in which the University processes your personal data, it is important that you are aware of your right to lodge a complaint with the Information Commissioner's Office by calling 0303 123 1113."

11. Who can I contact if I have further questions?

For any further questions please contact:

Principal Investigator: Cheylea Hopkinson at C.Z.L.Hopkinson@liverpool.ac.uk

Dissertation Advisor: Andrea Corradini at

[i] Review from an Animal Welfare and Ethical Review Body (AWERB) is usually required for any research which involves procedures that are carried out on any living vertebrate - other than man - and any living cephalopod and which are:

- not considered recognised veterinary clinical practice;
- not considered recognised agricultural practice;
- not considered animal husbandry practice;
- or covered precisely by an Animal Test Certificate under Veterinary Medicines Regulations.

[ii] Security Sensitive research includes, but is not limited to the commissioning, acquisitioning and communication with various groups, searching and downloading texts, videos and images that relate to:

- Terrorism and Counter Terrorism
- Extremism e.g. Al Qaeda, Jihadist, ISIS
- Religious
- Political
- UK Government/ Ministry of defence (MOD)
- Military/Weaponry/Explosives
- Nuclear

For more information please refer to the Oversight of security sensitive research materials.

[iii] Please visit the UK Caldicott Guardian Council website for information on the Caldicott principles

[iv] Please list all countries and research sites involved in the research.

[v] This includes any research which targets data collection from participants outside the UK, for example:

- All fieldwork conducted overseas (observations, interviews, surveys etc.)
- Any health-related research conducted overseas (clinical trials, human tissue collection, interventions, health-related surveys etc.)
- Online data collection (such as questionnaires, video interviews, chat room data etc.) that is specifically targeted at an overseas population

[vi] Resources on the various overseas research ethics committees can be found on the research ethics webpages (https://www.liverpool.ac.uk/intranet/research-support-office/research-ethics/).

[vii] For example - are the data protection laws similar to those in the UK, or are there important differences? Guidance on potentially relevant legislation in different countries can be found in the International Compilation of Human Research Standards.

[viii] For example: Are there any specific considerations with regard to approaching individuals? What are the normal practices for obtaining informed consent in this setting?

[ix] Please explain here the safety considerations outlined in your risk assessment, including:

- what training and support you received in order to carry out your research project overseas;
- whether advice from the Safety Office has been sought;
- what arrangements are in place to ensure that you will be receiving on-going supervision and oversight throughout your research project.

[x] Vulnerability is a fluid and contested term as there are many reasons why research participants may be disadvantaged. Vulnerability may result from factors such as the participants' sexual behaviour; their legal or political behaviour; their experience of violence; their gender or ethnic status; their age (e.g. children aged under 16); or their status in a dependent or unequal relationship. People may be vulnerable in different ways, and to different degrees at different points in their lives due to the circumstances in which they find themselves at a particular time. Vulnerability should not be seen as a characteristic of individuals or categories of people. It is important to recognise that prospective participants may be vulnerable, but not to assume they are vulnerable. Researchers should assess potential vulnerability within the context of the research.

[xi] The research aims should include: the background to your research; the research questions; any relevant existing literature.

[xii] This section should include details of: your methodology; the identification and recruitment of participants; details of how the data will be collected; how the data will be analysed.

[xiii] A reimbursement can be given to participants that acknowledges the time and effort they have provided in participating in the research or reflects any expenses that may occur I.e.- transport, parking, child care.

[xiv] Please do not write "No risk" or "Not applicable". Applications which do not adequately discuss the risks involved, will be returned to applicants. While the intention is not to fabricate or overstate potential risks, it should be recognised that all research involving human participants or personal data carries some risk, and applications should contain a constructive reflection on the likelihood and magnitude of risks. Potential risk to researchers may include:

- risk of physical threat or abuse
- risk of psychological trauma, as a result of actual or threatened violence or the nature of what is disclosed during the interaction
- risk of being in a comprising situation, in which there might be accusations of improper behaviour
- increased exposure to risks of everyday life and social interaction, such as road accidents and infectious illness

[xv] Please do not write "No risk" or "Not applicable". Applications which do not adequately discuss the risks involved, will be returned to applicants. While the intention is not to fabricate or overstate potential risks, it should be recognised that all research involving human participants or personal data carries some risk, and applications should contain a constructive reflection on the likelihood and magnitude of risks. Potential risk to researchers may include:

- Research topic: Is the topic of the study contentious and sensitive. How will you deal with this issue in your research project?
- Participants: Will the study will involve vulnerable people who might not be able to provide informed consent? What arrangements have you put in place to ensure that your participants fully understand the project and there is no coercion to participate?
- Recruitment of participants: Will participants in the study be approached in a public space? What matters arise from this research decision relating to the voluntary participation of people in the study and how have you addressed them?
- Confidentiality: Will you be able to offer confidentiality and anonymity to all your participants? What if they disclose illegal or potentially harmful information? Are they well known in their community? what if the answers they provide make them identifiable to other?

[xvi] It is good practice for researchers to provide feedback of the findings to research participants at the end of the study. The feedback usually covers:

- what participants can expect to happen to them at the end of a study;
- how those that have participated in the research can access the study results;
- how those who would rather not see the findings can opt out of the process, if this has not been covered already;
- who to contact if participants have any further questions;
- an acknowledgement of the contribution they have made to research.