A Work Project, presented as part of the requirements for the Award of a

Master’s Degree in Management / Finance from the

NOVA – School of Business and Economics

„The Impact of Blockchain Technology

on the Trustworthiness of Online Voting Systems

–

An Exploration of Blockchain-Enabled Online Voting“

Kevin Riedlberger – 34638

A Project carried out on the Master in Management / Finance Program,

under the supervision of:

Prof. Andrew Bell

Lisbon, 3 January 2020

„The Impact of Blockchain Technology on the Trustworthiness of Online Voting Systems – An Exploration of Blockchain-Enabled Online Voting "

Abstract

Online Voting evidently increases election turnouts. However, recent state-owned initiatives have failed due to security concerns and a lack of trust in the systems. Blockchain seems to be a very suitable technical solution to establish transparency in online voting and thus, create trust. We have built our own, blockchain-enabled voting platform and utilized it to run an A/B-testing experiment at an university election to investigate its effect. Our results which show that students trusted the blockchain-based voting version less than the control version can be found in Vysna (2020). The following discussion can be found in Konzok (2020).

Keywords: Blockchain, Online Voting, Trust, Transparency

This work used infrastructure funded by Fundacao para a Ciencia e a Tecnologia (UID/ECO/00123/2013, UID/ECO/00124/2019 and Social Sciences DataLab, Project 22209), POR Lisboa (LISBOA-01-0145-FEDER-007722 and Social Sciences DataLab, Project 22209) and POR Norte (Social Sciences DataLab, Project 22209).

Table of Contents

Table of Figures

Table of Tables

1. Introduction

According to Russell and Zamifir (2018), participation rates in parliamentary elections dropped by more than 10% globally between 1980 and 2018. To take countermeasures against this trend, online voting turned out to be a promising idea. Breux et al. (2017) found evidence that online voting actually increases election turnouts by especially encouraging less committed voters. Unfortunately, various, state-run initiatives to implement online voting have failed. The Netherlands forbade electronic counting of votes due to a strong fear of cyberattacks (Lowe, 2019) and France stopped all ongoing initiatives because of similar motivations (Reuters, 2018). The only exception remains Estonia, which already enabled online voting in parliamentary elections since 2005. In 2019, for the first time in history, it became the most popular channel to cast a vote with 44% of all participating voters using it (Krivonosova, 2019).

However, what seems to be missing to expand the implementation of online voting systems is the right technology. Both, the responsible authorities and the broad population have to trust their voting system to enable a successful transformation. Spycher et al. (2011) identified transparency as the most crucial factor for establishing trust in online voting systems. In achieving this, Dogo et al. (2018) stress that blockchain technology establishes strong perceived transparency. Our implied research hypothesis therefore states that introducing blockchain technology to online voting system does actually increase the trust in this system.

This hypothesis turns into our research question: To what extent the use of blockchain technology actually impacts the trustworthiness of online voting systems?

With the goal of investigating the answer, we built our own, blockchain-based online voting system, called Votechain, to run an expedient experiment. It technically works on a blockchain protocol and enables voters to cast their ballot online and verify it afterwards. Hereby, the voters are given access to the entire blockchain of the particular election they are participating in, in an encrypted manner. Each block represents one vote.

Votechain has been utilized in a students' elections encompassing almost 1000 votes out of which roughly every second student actively participated in our A/B-Testing experiment. The main goal of this experiment was to investigate, whether students who were prompted with a visualization of the election blockchain after they cast their vote would actually trust this online voting system more than the control group, to which state-of-the-art security methods were shown instead.

Our research paper starts off with an extensive literature review including an elaboration about the nature of elections, voting methods and the transition to online voting (Vysna, 2020), blockchain technology (Konzok, 2020) and blockchain-based voting (included in this paper). Thereafter, we describe Votechain and our experiment in the methods. The results and an adequate statistical analysis of our experiment can be found in Vysna (2020) and the following discussion is written down in Konzok (2020).

Individual Contribution

The literature review is split into three sections and represents the individual contributions to the master thesis of all of the team members. Nina Vysna created the first section — *Elections and trust* — and Ivo Konzok developed the second — *An exploration of blockchain technology* — which they submitted individually. The third section — *Blockchain-enabled online voting* — is written by Kevin Riedlberger and is part of the overall submission in this document.

2 Literature Review

2.1 Blockchain-enabled online voting

The other two literature review parts of Vysna (2020) and Konzok (2020) reflected on democratic elections in general and the blockchain technology. This part combines both of them and describes blockchain-enabled online voting systems. First, we compare traditional voting methods and online voting solutions in order to identify barriers that have prevented a large-scale adoption of the technology. Second, we examine what blockchain technology might offer to improve online voting systems. Third, several existing blockchain-enabled voting solutions are compared and contrasted. Ways in which these existing solutions are meeting election requirements will be explored individually. Fourth, we conclude why trust might be the crucial factor to assess the potential of blockchain-enabled voting systems and present our research hypothesis.

2.1.1 Comparison of traditional and online voting systems

For the following comparison the term *traditional voting schemes* refers to the paper ballot system because it reflects the current European standard (Russell and Zamfir, 2018).

First, a fundamentally important requirement for elections is accuracy of the vote count. While analysing different vote counting methods for traditional voting schemes, Goggin et al. (2012) observed a human error between approximately one and two percent. Causes of these errors include miscounting or misattributing votes due to poor handwriting. In contrast, electronic voting systems are based on a programmed logic, which prevents these problems (Willemson, 2017). However, a tampered voting machine may produce different results than an untampered machine while using the exact same input. The condition of dispute freeness stated by F.M.Mursi et al. (2013) is therefore in jeopardy for both of the two systems since both bear the risk of creating disputes (Willemson, 2017).

A second point of comparison is eligibility, which traditional voting schemes achieve by in-person authentication, often by providing identification (Paul et al., 2003). Online systems can either issue machine-readable identification cards or distribute unique identifiers to every voter via a secure channel like the postal system (Hill, 2016). In order to prevent voters from sharing their identification information with others, credentials can be substituted by biometric authentication techniques like fingerprints or iris scans, which are already in use in several African countries (Russell and Zamfir, 2018).

Third, privacy is a mandatory requirement in most democratic countries. It is satisfied by paper ballot voting because authentication and voting are separated processes, guaranteeing an anonymous vote while fulfilling the eligibility specification (Cuvelier et al., 2013). Internet voting schemes use encryption technology to provide privacy to its users (Hill, 2016). Hjálmarsson and Hreiðarsson (2018) presented one such method called the Zero-Knowledge Proof, which has become one of the most popular encryption methods for electronic voting systems. Closely connected to the privacy requirement is verifiability which can be further divided into universal and individual verifiability, as described in Vysna (2020). Achieving privacy and verifiability simultaneously is difficult since they tend to be mutually exclusive. While privacy requires the total separation between voter identity and the casted vote, verifiability needs to connect them (Jonker et al., 2013). Regarding paper ballot voting, both verifiability properties are practically unattainable in the majority of cases. Putting the vote into the ballot box, solely provides privacy and leaves the voter with trust in the central authority that the vote gets counted correctly (Cuvelier et al., 2013). Online voting schemes offer multiple solutions for both verifiability properties which are also able to provide their voters privacy, as can be seen in the research of Hill (2016).

A major challenge of the transition from traditional to internet voting schemes is to ensure uncoercibility which Krivoruchko (2007) describes as the ability to protect voters from any influence by coercers. Conventional voting booths can prevent coercion by having individuals vote privately. While not a perfect system — for example, individuals can still be threatened or blackmailed to vote a certain way — private voting booths are an effective countermeasure against coercion. As soon as the voting itself is carried out remotely, coercion becomes a serious threat because attackers are able to extend their reach and data collection opportunities (Juels et al., 2010). Also established methods like postal voting leave the voter vulnerable to coercible approaches from others (Hill, 2016). As any remote voting scheme, online voting systems bear the same risk and cannot provide the same protection against coercion as private voting booths in polling stations (Valenty and Brent, 2000). But some of the online systems provide methods to counteract coercion. For example, the Estonian online voting solution allows their citizens to vote an unlimited amount of times, overturning the earlier votes each time (Russell and Zamfir, 2018). As a result, Estonian voters can alter an earlier, coerced vote. In summary, online voting systems actually comply with five out of six of the regarded criteria whereas, by this framework, traditional systems actually lack three out of six. The only requirement not fulfilled by online voting systems is dispute freeness which is not fulfilled by traditional systems either. The primary reason for the hesitant implementation of online voting systems is prevalent security concerns. Policymakers and voters fear the systematic fraud. Specifically, concerns surround being electronically spied on, or voters being tampered with by hackers (Susskind, 2017).

Apart from the conducted comparison regarding election requirements, online voting systems might contain the potential to lower costs and improve voter turnout. While analysing the Estonian internet voting system, Krimmer et al. (2018) calculated cost savings of approximately 50% compared to the second cheapest option of the election, represented by traditional polling stations. The effect on turnout is more difficult to determine. While Sál (2015) concluded that the online system was accepted rapidly by the majority of the Estonian population and increased turnout slightly, similar research of Germann and Serdült (2017) showed that the implementation of internet voting in Switzerland for referendums did not increase voter turnout. The latter study stressed that the effect on turnout is dependent on the existing voting infrastructure, since Switzerland had a well-established postal voting system in place which offered its citizens to vote remotely even before the internet voting alternative.

2.1.2 Why blockchain technology might improve current online voting systems

One subset of internet voting systems is blockchain-based voting technology. In order to justify the potential of a blockchain-based system for hosting elections, it should meet the standards of existing online voting systems while providing further improvements, specifically regarding security (Wolf et al., 2011), trustworthiness and transparency. As described in Vysna (2020), Moynihan (2004), F.M.Mursi et al. (2013) and Gritzalis (2012) identify a collection of flaws in currently used voting schemes including tampering, residual votes, errors of optical scanners and machines in general. Considering these issues, blockchain technology provides immutability, durability and "eliminates single points of failure" (Abeyratne and Monfared, 2016, p.3). In regular online voting systems, such single points of failure are represented by their centrally controlled database. Since a successful cyberattack would result in a large data loss, the public is forced to trust the central authority to keep the records accurate (Lewis et al., 2017). Blockchain decentralizes the database across its network. Utilizing the consensus protocols, explained in chapter two, this enables everyone to verify the correctness of the count and ensures that no data has been altered, deleted or entered without authorization (Hanifatunnisa and Rahardjo, 2017). In order to remove blockchain's integrity, malicious attackers would have to own a majority of nodes as explained by Tosh et al. (2017). Since the blockchain protocol is open-source, the voters can be certain that the system runs as intended based on its source code (Abeyratne and Monfared, 2016). While bearing the risk that potential vulnerabilities of such a system can be exposed, providing the code as open source also enables the public to find solutions and improvements for security problems (Volkamer et al., 2011). Thus, dispute freeness can also be achieved, which lets blockchain-based election systems fulfill all aforementioned criteria. Combining all those features, blockchain technology is able to provide online voting systems a high level of transparency regarding the electoral process which is necessary for a healthy democracy (Susskind, 2017).

2.1.3 Existing concepts of blockchain-enabled voting systems

After exploring the potential of blockchain technology for electoral systems, this section introduces existing blockchain-based election systems, created by different corporations.

Highlighted here are unsolved challenges, presented by analysing how each corporation's technology performs according to the aforementioned, predetermined election requirements.

2.1.3.1 Overview of current blockchain-based voting applications

Cucurull et al. (2019) summarized seven well-known online voting applications which are using blockchain technology. Due to the limited publicly available information about those applications, their websites and white papers are the only resources in most cases. Hayes (2019) defined a white paper as an "...informational document, usually issued by a company or not-for-profit organization, to promote or highlight the features of a solution, product, or service". When using them as a source of information about a technology, it should be mentioned that they are often used as a marketing tool and thus, highlight the positive aspects of each application. Appendix 1 presents a detailed overview of the seven applications, analysed by Cucurull et al. (2019) and compares their individual blockchain infrastructure, encryption technology, unique features, business model and funding.

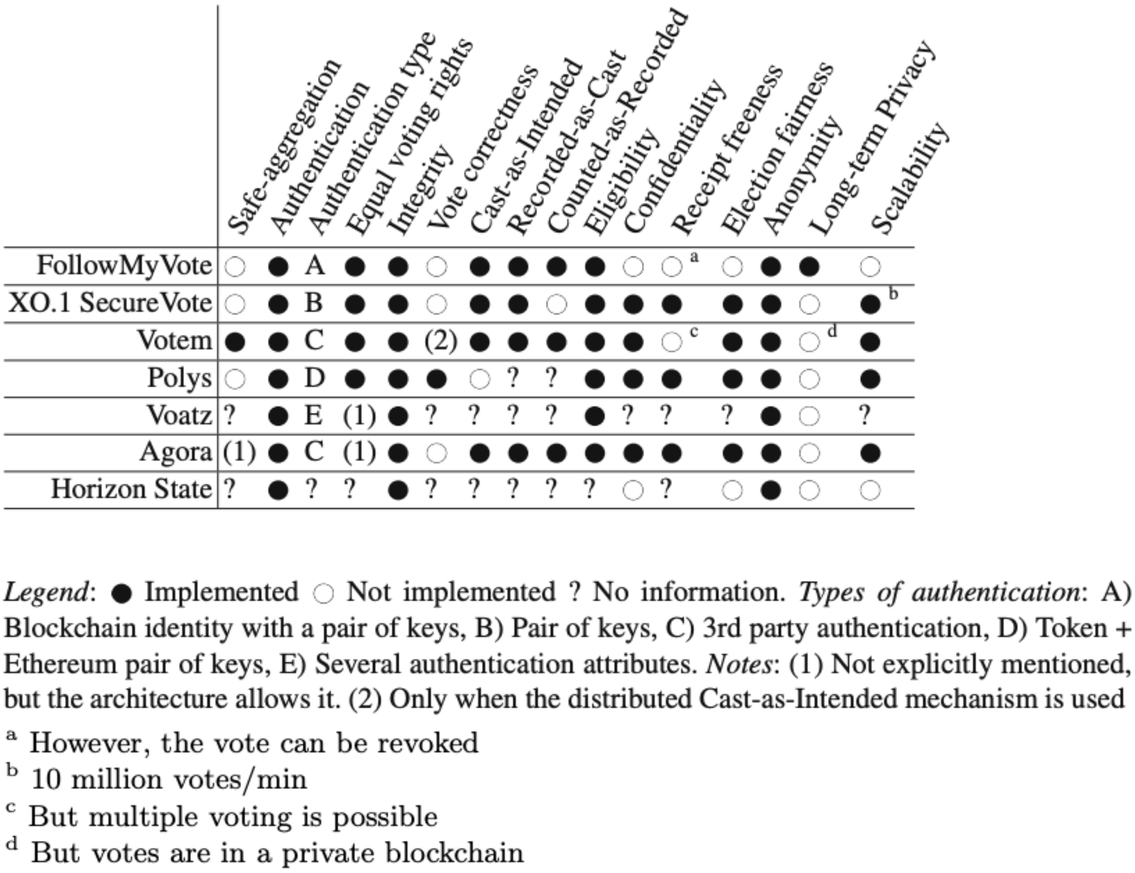
While the applications differ significantly from each other in many aspects, they are united by the attempt to "provide verifiable integrity while minimizing privacy loss" (Bernhard et al., 2017, p.88), using blockchain technology. The majority of applications focus on large-scale projects, which are ordered on-demand by customers like universities, organizations, local and national governments. Besides paying the firms directly for carrying elections out utilizing their applications, clients can also purchase each company's tokens which are publicly traded on cryptocurrency exchanges such as *binance.com*. These tokens get distributed to the voters and have to be spent in order to authenticate users or cast ballots during the election. Out of the four businesses (FollowMyVote, Votem, Agora and Horizon Sate) basing their system on tokens, only Agora's *VOTE* (Binance, n.d.) and Horizon State's *Decision Token* (CoinMarketCap, n.d.) can currently be purchased and are traded publicly. It should be mentioned, however, that Horizon State closed for business on August 19th, 2019 due to a lawsuit. This again illustrates the unpredictability of the yet immature cryptocurrency-based market (Campbell, 2019).

The investments of venture capitalists into companies building on blockchain technology have been increasing (CB Insights, 2018) and firms like Medici Ventures start to focus solely on funding such startups, for example Voatz and Votem (Medici, n.d.). Regarding successful real-life experiments, the majority of the systems have already supported numerous elections of several customers varying from universities, municipals, companies, conferences, labor unions and governments. These successful real-life experiments ranging between a couple of hundred votes, up to 1.8 million votes (Votem, 2017a), along with the increasing amount of investments in these systems, show that there is a general interest in blockchain-based voting schemes from the public.

2.1.3.2 The effectiveness of current blockchain voting systems

The presented voting applications show a high diversity in their approaches to build a secure voting system. Cucurull et al. (2019) analysed the extent to which they meet international standards, specifically the recommendations of the Council of Europe from 2017 (Committee of Ministers, 2017). The authors added a set of requirements, which are stressed Vysna (2020) and chapter 2.1.1. These are accuracy (vote correctness), eligibility, privacy, integrity, authentication, verifiability and uncoercibility. Moreover, the authors included long-term privacy and scalability. Table 3 provides a summary of this comparison.

Table 1: Properties of selected blockchain-based voting systems (Cucurull et al., 2019, p.309)



	Safe-aggregation	Authentication	Authentication type	Equal voting rights	Integrity	Vote correctness	Cast-as-Intended	Recorded-as-Cast	Counted-as-Recorded	Eligibility	Confidentiality	Receipt freeness	Election fairness	Anonymity	Long-term Privacy	Scalability
FollowMyVote	○	●	A	●	●	○	●	●	●	●	○	○[a]	○	●	●	○
XO.1 SecureVote	○	●	B	●	●	○	●	●	○	●	●	●	●	●	○	●[b]
Votem	●	●	C	●	●	(2)	●	●	●	●	●	○[c]	●	●	○[d]	●
Polys	○	●	D	●	●	●	○	?	?	●	●	●	●	●	○	●
Voatz	?	●	E	(1)	●	?	?	?	?	●	?	?	?	●	○	?
Agora	(1)	●	C	(1)	●	○	●	●	●	●	●	●	●	●	○	●
Horizon State	?	●	?	?	●	?	?	?	?	?	○	?	○	●	○	○

Legend: ● Implemented ○ Not implemented ? No information. *Types of authentication*: A) Blockchain identity with a pair of keys, B) Pair of keys, C) 3rd party authentication, D) Token + Ethereum pair of keys, E) Several authentication attributes. *Notes*: (1) Not explicitly mentioned, but the architecture allows it. (2) Only when the distributed Cast-as-Intended mechanism is used

[a] However, the vote can be revoked
[b] 10 million votes/min
[c] But multiple voting is possible
[d] But votes are in a private blockchain

Starting with accuracy or correctness, Cucurull et al. (2019) used a different definition, solely focusing on providing the user feedback if there is an error casting their vote. We will base our analysis on the definition given by Lambrinoudakis et al. (2003) which is used in Vysna (2020) for the sake of continuity within this project. They define an election as accurate if all valid votes are included in the final count and cannot be changed by anyone. According to chapter 2.1.1, all electronic voting systems are fulfilling the accuracy requirement. Eligibility, authentication and privacy which Cucurull et al. (2019) calls anonymity are provided by all the applications, as well as integrity which is fulfilled by blockchain technology by default (Abeyratne and Monfared, 2016). The verifiability requirement is redefined for end-to-end online voting systems into three parts, namely cast as intended, recorded as cast and tallied as recorded. Thus, voters can verify if their ballots were marked correctly, recorded correctly and if the overall voting result is correct (Wu, 2018). Due to a lack of information provided by the companies running the regarded applications, the analysis for verifiability is not complete but the overall accessible information suggests that the applications are satisfying the verifiability requirements (Cucurull et al., 2019). Finally, reviewing the individual white papers of the applications leads to the conclusion that besides SecureVote, none of the systems addresses coercion. SecureVote is offering its users the possibility to generate a receipt of a fake vote which makes it impossible for a third party to identify if the receipt the voter has shown is correct or fake (Cucurull et al., 2019).

In addition, Cucurull et al. (2019) reviewed two more properties, namely long-term privacy and scalability, which are specifically important for blockchain-based voting schemes. Long-term privacy refers to the application's ability to disconnect voter identities from their casted votes in the long-term. This sense of anonymity is in most of the regarded applications secured by combining key-sharing schemes and encryption. Underlying current computational power benchmarks, this principle works reliably, however, future improvements of computational power could jeopardize these encryption algorithms and expose voter identities. Regarding the seven applications, only FollowMyVote claims to use a technique to ensure voter privacy which works independently of the level of computational power and thus, provides robust long-term privacy. Secondly, the scalability of applications is taken into consideration. Bitcoin (seven transactions per second) and Ethereum (20 transactions per second) lack a sufficiently high level of scalability, as it is explained Konzok (2020) (Chauhan et al., 2018). As a result, FollowMyVote and Horizon State, being based on these two blockchains respectively, fail to qualify for running high level elections (Cucurull et al., 2019). The other systems fulfill the requirement because their systems either work on scalable, private or permissioned blockchains or develop their own sophisticated hybrid like SecureVote. In the latter option, this hybrid stacks the collected votes into immutable and digital pallets before sending them to the blockchain. Thus, the number of transactions is reduced which ultimately provides a high level of scalability.

In conclusion, existing blockchain-based online voting systems fulfill the majority of technical properties but are not yet considered to be mature enough for large-scale adoption.

2.1.4 Trust as a deciding factor and our research question

People's trust in the electoral integrity is fundamental for democratic elections, as it is discussed in Vysna (2020). Hence, the decision of whether to implement a new online voting system or not should not only be based on its technological properties but also on the public's perception of it, since "a voting system is only as good as the public believe it to be" (Mc Galey and Paul Gibson, 2003, p.4). This is consistent with the findings of Vassil et al. (2016), where the authors identified that Estonian voters who trust in the internet voting system were more likely to vote online than people who considered it less trustworthy. Blockchain technology offers a promising alternative to increase electoral integrity by design. Instead of attempting to build more confidence in a central authority controlling the process, the blockchain substitutes trust with cryptographic proof (Nakamoto, 2008). Existing blockchain-enabled voting applications argue that this makes trust in electoral authorities obsolete. In exchange, it requires voters to put their trust into the procedure itself, which is completely transparent as it provides an auditable source code and the possibility of vote verification (Agora, 2015; Horizon State, 2017; Polys, 2017). The Council of Europe (2011) agrees that the key to build public trust in online voting systems, is to make the process transparent and to openly communicate the reasons for its introduction. At the same time, the Council questions if the public will be able to understand the technology. Boucher (2017) supports this concern by pointing out blockchain's complexity as a possible barrier to general acceptance. Hill (2016) provides corresponding evidence for this claim since existing, sophisticated methods like Zero-Knowledge Proof or MixNet which solve specific online voting issues are still not implemented at larger scale due to a lack of understanding. Certain countries, such as Germany, even legally require that every voter has to be able to observe, understand and verify the voting scheme, based on the latest German Constitutional Court decision in 2009 (Seedorf, 2016). Lacking the ability to distinguish between blockchain-enabled voting systems and regular internet voting solutions and to understand the advantages blockchain offers, could lead to the same trust issues the public has towards online voting mechanisms in general (Susskind, 2017).

Although plenty of research has been conducted, addressing if blockchain technology can improve internet voting from a technical perspective, the question remains, whether voters consider blockchain-enabled voting applications more trustworthy than regular online voting systems. Therefore, the goal of this study is to empirically assess the difference in perceived trust of voters in the voting procedure between those who use a regular online voting system and those who vote on a blockchain-enabled solution. Based on the technical advantages blockchain offers regarding security and transparency, it is hypothesized that:

Utilizing blockchain technology will lead to an increase of voter's trust in online voting.

Group Contribution

The overall project was carried out by three students and is submitted individually which also includes the personal group contributions to the final document. Included in this part of the project is the methods section. The individual work of Nina Vysna — *Elections and trust* — contains the results section and Ivo Konzok's work — *An exploration of blockchain technology* — contains the discussion section.

3. Methods

3.1 Experimental Design

To test our hypothesis, we designed a randomized controlled trial experiment. Such an experiment entails randomly assigning the subjects in one of the two groups: *experimental/treatment group* that receives the tested intervention and *control group* that receives alternative treatment. Afterwards, the two groups are surveyed in order to determine if there is a difference between them in the outcome and thus if the applied intervention had the desired effect (Kendall, 2003).

In the context of websites and applications, such an experiment is also called A/B testing. A/B testing is a method that allows for comparing two versions of a website and evaluating which version performs better. In our case, version A, shown to the control group was a simple online election website with state-of-the-art two factor authentication and version B, shown to the experimental group was a blockchain enabled voting system in which voters were able to see every cast vote as a block in a blockchain. We alternated A and B version for each voter to achieve an approximately equal distribution of voters in each group. Section 3.2 describes the technical and design differences between the two versions in more detail and section 3.3 explains further details of the experiment and the used measures.

3.2 Description of the online voting system

To execute the A/B testing and investigate how the use of blockchain technology influences the trustworthiness of online voting systems, we started by building our own, blockchain-based online voting application called Votechain. This application enabled us to run the experiment while deploying it on the Students Representative Election for the Pedagogical Council on the 13th of November 2019 at Nova School of Business and Economics. The election consists of five sub-elections, one for PhD students (95), three for different master's degrees (1638) and one for bachelor students (1394), which contains a total of 3129 eligible student voters. Following up on pursuing an open-source approach, we developed the application's backend in Python and connected it to a PostgreSQL database. Python enabled us to leverage already existing third-party modules, especially regarding all functionalities directly related to the blockchain. PostgreSQL provided advanced query optimization and locking mechanisms which made sure the blockchain did not fork over the course of the election. To deploy Votechain, we used the Flask web framework due to its high flexibility and speed. For a more detailed look at the backend processes, please have a look at appendix 2 or find the whole source code of the application in our GitHub repository, linked in appendix 3. According to Iansati and Lakhani (2017), blockchain-based applications should have the same standard of practicality and functionality as existing applications they try to replace. Therefore, our web design approach aimed at creating a very simplistic and intuitive voting experience for the user which is illustrated in appendix 4. The whole process of Votechain is explained in the following.

Prior to the elections, all students were informed about the online voting system and received its URL which guided them to the website. Before entering the actual voting procedure, the first step on the website required the users to successfully authorize themselves. Nova SBE uses Google's Gmail service for all its student accounts which led us to integrate Google Sign-in. The API checked if the entered credentials are correct and identify a Nova SBE user. Importantly, this ensured only currently enrolled Nova SBE students could vote in the elections, avoiding any sample contamination. After a successful login, the application accessed the database and compared the credentials with the official white list. The admission was only allowed in case the user was eligible to vote in one of the published elections.

Once the users completed the authorization, they were redirected to the first of two pages. Screenshots of the entire user experience can be found in appendix 5-7. First, users saw the voting page. The voting page displayed the corresponding election with respect to their program including all required information for each voter such as a short description of the election itself and their candidate lists. We used a step-by-step design approach to guide the user through the process in order to avoid any confusion. Each step contains a maximum of two sentences and requires only one interaction. Step one lets voters select their candidates list of choice and step two lets them submit it. To further minimize any issues like accidental selections, we implemented a third step where the users could see their selected list again and had to confirm it before the vote was ultimately counted. Up until this point, every voter experienced exactly the same universal voting procedure. By confirming their vote, the users were redirected to the second page: the verification page.

On the verification page, we introduced the A/B testing by creating two different versions of the page. Both versions followed the same step-by-step design as before and both were based on the same overall structure. The first step provided the users a randomly generated password which they were instructed to save on their local devices in order to verify their vote later on. The second step informed the voters briefly about the security features of the system and in the third step they were able to verify their vote. By entering the password, they received earlier, all relevant information about their cast vote was revealed. Eventually, step four redirected them to the survey. All functionalities of the verification page remained available during the entire time frame of the election and beyond. While consisting of the same parts, the two versions differed in their specific content within the first three steps. While version B clearly communicated and emphasized its underlying blockchain technology, version A represented a state of the art online-voting-system, which deliberately did not mention blockchain-related content. In specific, the differences are listed in the following table:

Table 2: Content differences between version A and version B of the online voting system

	Version A	**Version B**
Step 1: ***Voting Credentials***	The private key is called 'Password'.	The private key is called 'Voter Key'. It is mentioned that the system is running on a blockchain.
Step 2: ***Security Features***	Emphasis of the integrated two-factor-authentication method of the system and a brief explanation of it. This should provide a comparable sense of security for the users. It is repeatedly pointed out to store the password since the system will not store it to enhance privacy.	Visualization of the entire blockchain and a brief explanation of its basic logic in the context of an election. The user is able to scroll through all numbered votes and their information (hash, previous hash, from address and timestamp). It is repeatedly pointed out to store the Voter Key since the system will not store it to enhance privacy.
Step 3: ***Verify Your Vote***	The Private Key is called 'Password'. If a user enters the private key correctly, the displayed vote contains the selected candidate list and timestamp as information.	The Private Key is called 'Voter Key'. If a user enters the private key correctly, the displayed vote contains the hash, previous hash, from address, to address, selected candidate list and timestamp as information.

A more detailed explanation regarding the different components of a block can be found in appendix 8. Once the election was over, the blockchain additionally displayed the 'to address' of each vote. This was highly significant to the transparency of blockchain because it allowed voters to theoretically prove the public count by tallying the votes on their own. Note that this information was not visible to voters until after the election to fulfil the fairness property, described in chapter 2.1.1 (knowing the vote count of an ongoing election could influence the decision of voters). By the design of the experiment, the two versions displayed different information, but both offered the users the exact same functionalities.

3.3 Survey

3.3.1 Measures

As mentioned above, the last step of the verification page was an invitation to fill in the survey that we used to measure the outcomes of the treatment. We used the survey software Qualtrics to build and administer a web survey to collect data from undergraduate and graduate students at Nova SBE on the 13th of November, the day of the campus wide elections for next year's Student Representatives. Students were notified about the upcoming elections a week prior to the election day, one day prior to the election day and three times on the election day itself. The elections were held solely via our web application; the paper ballot option used in previous years was eliminated.

We chose the students of Nova SBE as our subjects because the mentioned elections that are held annually presented a unique opportunity to perform the trial with up to 3127 subjects and thus obtain large enough sample.

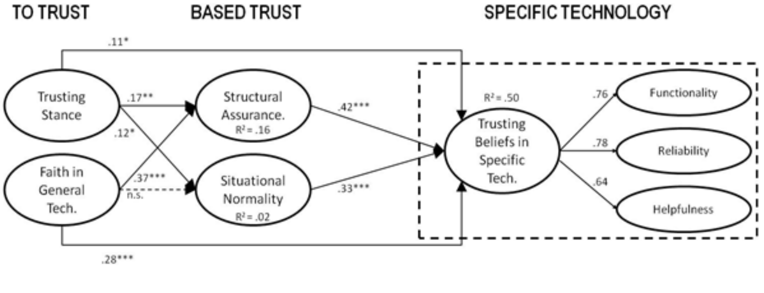
Using an online survey enabled us to collect responses from our subjects right after they used the voting application, ensuring that the experience was easy to be recapitulated. As suggested by Dillman (2007), cash and non-cash incentives can increase the response rate of web-based surveys. Therefore, we encouraged subjects to fill in the survey by offering an incentive that one randomly drawn respondent would receive a dinner voucher for four people in a local restaurant.

The questionnaire (reported in Appendix 9) consisted of 32 questions in total, with 25 questions measuring trust on three different layers, five demographic questions regarding gender, age, race, nationality and university program the subjects were enrolled in, and two optional questions. The last two optional questions asked subjects to state their email address if they would have liked to be contacted, in case they won the prize. They were also able to indicate if they would like to participate in a focus group.

Measures used in the questionnaire were adapted from the study by McKnight et al. (2011). These researchers developed and empirically tested constructs that measure trust in technology on three different levels. We were comfortable using these measures as the authors reported strong reliability (Cronbach's alpha > 0.89), convergent validity and discriminant validity. As opposed to other researchers who attempted to measure the same concept, they focused on trust in the technology itself rather than focusing on human traits found in technology. As suggested by Knight et al. (2011), this approach allows to determine “what is it about technology that makes the technology itself trustworthy, irrespective of the people and human structures that surround the technology” (p.2). However, they also argue that trust in technology is fairly similar to trust in people as trusting both people and technology involves risk, uncertainty and dependence on another. Therefore, they developed the measures for trust in technology as an analogy to already existing measures of trust in people.

The survey is composed of three constructs that reflect the three levels of trust: a) propensity to trust general technology; b) institution-based trust in technology and c) trust in specific technology. These constructs consist of several sub-constructs as displayed in Figure 5 below. The researchers found significant direct relationships between the sub-constructs belonging to the respective constructs. This signals that if one wants to fully understand the sources of trust in specific technology, it is useful to include propensity to trust general technology items and institutions-based trust items. Hence, we included all three constructs and thus seven sub-constructs each measured by three to four Likert scale items in the survey. Constructs’ scores are calculated as the averages of their subconstructs’ scores.

Figure 1: Structural Model of Relations among Trust Constructs (McKnight et al. 2011, p.10)



Propensity to trust in general technology is an individual's willingness to depend on technology across different situations and technologies. It is made up of two sub-constructs: a) faith in general technology - an individual's beliefs about the reliability, functionality and helpfulness of information technologies in general and b) trusting stance - an individual's beliefs about a positive outcome stemming from relying on IT. Both sub-constructs are measured with three to four Likert scale items in the survey.

Institution-based trust reflects the beliefs about the performance of a specific class of technologies in a particular context. It is composed of two sub-constructs: a) situational normality - a belief that using a specific class of technologies in a different way is perceived as normal within a certain context; and b) structural assurance - a belief that there is a necessary legal, contractual or physical support available for the class of technology that ensures the success of this technology. Each sub-construct is measured with four Likert-scale items in the survey.

The most crucial construct for our research is trusting beliefs in a specific technology that “reflect beliefs that a specific technology has the attributes necessary to perform as expected in a given situation in which negative consequences are possible” (McKnight et al. 2011, p.5). This construct is reflected in three dimensions: a) reliability – belief that the technology will consistently operate properly, b) functionality - belief that the technology has the capability to complete a task and c) helpfulness - belief that the help function is adequate. Each of these dimensions is measured by three to four Likert scale items. According to the authors, the construct exists on a deeper level than its dimensions. In other words, trusting beliefs in a specific technology are not an aggregation of the beliefs about reliability, functionality and helpfulness. Rather, if one trusts a specific technology, this will be reflected in an increase in trusting beliefs regarding the three dimensions.

The survey questions were formulated as similar as possible to the original measures. However, it was necessary to adapt them slightly to fit our research purpose. Trust in general technology construct remained unchanged. The class of technology questioned in the items belonging to the institution-based trust construct has been changed to *online voting systems.* The specific technology mentioned in the items belonging to the trusting beliefs in specific technology construct was naturally our voting application, Votechain.

3.3.2 Analysis

The measures we adopted in the survey proved to be reliable; Cronbach's alpha was above the recommended threshold of 0.70. Furthermore, principal component analysis verified that the items belonging to the same sub-construct correlate well with each other. After this initial analysis of the used measures that confirmed their suitability for our research, we assessed the sample for any demographic imbalances using a two-tailed t-test to compare the proportions of each demographic in the control and the treatment group. We found a significant imbalance in terms of gender and race (white and black in specific). Due to the imbalance, we were not able to perform a simple t-test to examine the difference in trust between the groups. Instead, we used multiple regression analysis and controlled for the imbalanced variables.

The first model uses the mean scores for constructs and sub-constructs as dependent variables and gender and race as control variables. The key independent variable of interest is *treatment* which is equal to 0 if voter belongs to the control group and 1 if voter belongs to the treatment group. The regression model specification is given by:

$$(1)\ construct = \beta_0 + \beta_1 \cdot female + \beta_2 \cdot black + \beta_3 \cdot asian + \beta_4 \cdot other\ race + \beta_5 \cdot treatment + \varepsilon$$

where *construct* is the participant's mean score for the items belonging to a construct or sub-construct. In total, we ran this model 10 times: once for each of the seven sub-constructs (reliability, functionality, helpfulness, situational normality, structural assurance, faith in general technology and general stance towards technology), and once for each of the three constructs (trusting beliefs in specific technology, institution based trust and propensity to trust general technology).

We further developed three additional models that attempt to measure the added effect of some of the demographic variables on the constructs by adding interaction terms in our model. Specifically, we explored if gender (female, male), nationality (Portuguese, German, Italian, other), and the program (masters, bachelors, PhD.) have any additional effect (on top of the treatment) on the dependent variables. Since the sample was quite uniform in terms of race and age, we did not include the interaction variables that capture the added effect of these variables. In addition, we split the sample based on the voters' mean score for the construct propensity to trust general technology into three groups: voters with high general technology trust (mean >= 4.5), neutral general technology trust (3.5<mean<4.5) and low general technology trust (mean<3.5). Similarly, the sample was split based on the scores for institution-based trust. We included these variables in the models to verify the findings of McKnight et al. (2011) who found that propensity to trust in general technology sub-constructs have direct relationship with sub-constructs of institution based trust as well as trust in specific technology; and subconstructs of institution based trust have direct relationship with the trust in specific technology (as pictured in Figure 2).The second model is specified as follows:

$$(2)\ construct = \beta_0 + \beta_1 \cdot female + \beta_2 \cdot black + \beta_3 \cdot asian + \beta_4 \cdot other\ race + \beta_5 \cdot German + \beta_6 \cdot Italian + \beta_7 \cdot other\ nationality + \beta_8 \cdot bachelors + \beta_9 \cdot Ph.D. + \beta_{10} \cdot other\ program + \beta_{11} \cdot gen.tech.neutral + \beta_{12} \cdot gen.tech.low + \beta_{13} \cdot instit.tech.neutral + \beta_{14} \cdot instit.tech.low + \beta_{15} \cdot treatment + \beta_{16} \cdot female \cdot treatment + \beta_{17} \cdot German \cdot treatment + \beta_{18} \cdot Italian \cdot treatment + \beta_{19} \cdot other\ nationality \cdot treatment + \beta_{20} \cdot bachelors \cdot treatment + \beta_{21} \cdot Ph.D. \cdot treatment + \beta_{22} \cdot other\ program \cdot treatment + \beta_{23} \cdot gen.tech.neutral \cdot treatment + \beta_{24} \cdot gen.tech.low \cdot treatment + \beta_{25} \cdot instit.tech.neutral \cdot treatment + \beta_{26} \cdot instit.tech.low \cdot treatment + \varepsilon$$

where *construct* represents the participants mean scores for the construct trusting beliefs in specific technology and its sub-constructs (reliability, functionality, helpfulness). We ran this model four times, once for each construct/sub-construct.

The third model is specified by:

$$(3)\ construct = \beta_0 + \beta_1 \cdot female + \beta_2 \cdot black + \beta_3 \cdot asian + \beta_4 \cdot other\ race + \beta_5 \cdot German + \beta_6 \cdot Italian + \beta_7 \cdot other\ nationality + \beta_8 \cdot bachelors + \beta_9 \cdot Ph.D. + \beta_{10} \cdot other\ program + \beta_{11} \cdot gen.tech.neutral + \beta_{12} \cdot gen.tech.low + \beta_{13} \cdot treatment + \beta_{14} \cdot female \cdot treatment + \beta_{15} \cdot German \cdot treatment + \beta_{16} \cdot Italian \cdot treatment + \beta_{17} \cdot other\ nationality \cdot treatment + \beta_{18} \cdot bachelors \cdot treatment + \beta_{19} \cdot Ph.D.\cdot treatment + \beta_{20} \cdot other\ program \cdot treatment + \beta_{21} \cdot gen.tech.neutral \cdot treatment + \beta_{22} \cdot gen.tech.low \cdot treatment + \varepsilon$$

in which *construct* is the participants mean score for the construct institution-based trust and its sub-constructs (situational normality, structural assurance). Variables *low institutional trust* and *neutral institutional trust* and their interactional terms with treatment variable are left out since institution-based trust is captured in the dependent variable in this model. We ran this model three times, once for each construct/sub-construct.

Finally, the fourth model:

$$(4)\ construct = \beta_0 + \beta_1 \cdot female + \beta_2 \cdot black + \beta_3 \cdot asian + \beta_4 \cdot other\ race + \beta_5 \cdot German + \beta_6 \cdot Italian + \beta_7 \cdot other\ nationality + \beta_8 \cdot bachelors + \beta_9 \cdot Ph.D. + \beta_{10} \cdot other\ program + \beta_{15} \cdot treatment + \beta_{16} \cdot female \cdot treatment + \beta_5 \cdot German \cdot treatment + \beta_6 \cdot Italian \cdot treatment + \beta_7 \cdot other\ nationality \cdot treatment + \beta_8 \cdot bachelors \cdot treatment + \beta_9 \cdot Ph.D.\cdot treatment + \beta_{10} \cdot other\ program \cdot treatment + \varepsilon$$

where *construct* is the participants mean score for the construct propensity to trust general technology and its sub-constructs (faith in general technology, stance towards general technology). Variables *low general technology trust* and *neutral general technology trust* and their interaction terms with treatment variable are left out since trust in general technology is captured in the dependent variable. *Low institutional trust* and *neutral institutional trust* variables and their interaction terms with treatment are also left out since, according to McKnight et al. (2011), propensity to trust technology in general technology has an impact on institution-based trust, rather than vice versa.

3.4 Focus Group for gathering qualitative feedback

In addition to the survey and its quantitative measurement of trust, we also decided to set up a focus group to gather qualitative feedback from users to elucidate our quantitative findings from the survey. More precisely, we intended to gain insights about voter's general attitude towards online elections, their knowledge about blockchain and their opinion about the provided system for the student representative elections in particular. Seven of the students who consented to participate in the survey were randomly selected to participate in the focus group. The date for the meeting was set to the following Monday (five days past the election) to ensure that the participants could still remember most details of their experience. The whole research team was present during the discussion. The team initiated the discussion and guided the participants through the protocol of six main questions. The attendees were encouraged to share their opinion with the group, to be critical and to discuss beyond the stated questions whenever they felt like a crucial argument was left out. After the focus group finished, the research team transcribed the recording. The complete transcription can be found in appendix 10.

4. Conclusion

Blockchain bears high potential to enhance the transparency of online voting systems and therefore increase their trustworthiness to drive adoption and higher election turnouts. We expected that our A/B-experiment would reveal higher levels of trust for blockchain-enabled voting in contrast to a two-factor-authentication security protocol, which we used for the control group of our experiment. Our results showed the opposite. Although only one of the seven sub-constructs we applied to measure trust showed a significant difference between version A and B, this difference was in favor of two-factor-authentication. Students tended to perceive version A (two-factor-authentication) as more reliable than version B (blockchain-based) (Vysna, 2020). However, we were able to retrieve from literature that transparency of online voting systems and familiarity with the utilized technology are key enabler of trust, which is supported by our focus group findings. Students agreed that blockchain enhances transparency which verifies the technology's potential for being applied in online voting.

Therefore, we concluded that people have to become more familiar with blockchain technology to be able to trust its application. The right way to achieve a widespread technical understanding seems to be educating the population ahead of time. Future research should use our findings to set up an experiment, using a representative sample and effective education methods, to fundamentally approve blockchain's potential in driving the trustworthiness of online voting systems. In times of decreasing turnouts of parliamentary elections and a dangerous shift to the right in global politics, the importance of finding effective ways to engage people in raising their political voice cannot be overstated (Konzok, 2020).

5. Bibliography

Abeyratne, S. A., and R. P. Monfared. 2016. “Blockchain Ready Manufacturing Supply Chain Using Distributed Ledger.” *International Journal of Research in Engineering and Technology* 05 (09): 1–10.

Agora. 2015. “Agora - Bringing Our Voting Systems into the 21st Century.” Agora. https://static1.squarespace.com/static/5b0be2f4e2ccd12e7e8a9be9/t/5b6c38550e2e725e9cad3f18/1533818968655/Agora_Whitepaper.pdf.

Agora. 2018. “Swiss-Based Agora Records First Government Election on Blockchain as Accredited Observer in Sierra Leone.” Medium. AgoraBlockchain. March 9, 2018. https://medium.com/agorablockchain/swiss-based-agora-powers-worlds-first-ever-blockchain-elections-in-sierra-leone-984dd07a58ee.

Bernhard, Matthew, Josh Benaloh, J. Alex Halderman, Ronald L. Rivest, Peter Y. A. Ryan, Philip B. Stark, Vanessa Teague, Poorvi L. Vora, and Dan S. Wallach. 2017. “Public Evidence from Secret Ballots.” In *International Joint Conference on Electronic Voting*, 84–109. Springer.

Binance. n.d. “Binance: VOTE Token.” Binance. Accessed September 12, 2019. https://www.binance.org/en/trade/VOTE-FD4_BNB.

Boucher, P., Nascimento, S. & Kritikos, M., 2017. How blockchain technology could change our lives. *STOA*.

Breux, Sandra, Jérôme Couture, and Royce Koop. 2017. “Turnout in Local Elections: Evidence from Canadian Cities, 2004–2014.“ Canadian Journal of Political Science 50(3), 699-722. doi:10.1017/S000842391700018X.

Campbell, Rebecca. 2019. “Blockchain Voting Platform Horizon State Shuts down after Lawsuit.” Yahoo Finance. August 21, 2019. https://finance.yahoo.com/news/blockchain-voting-platform-horizon-state-140552054.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAE-N7ljAtRtwITGk_-m20Zkj9rMVGRkNLb0IlaZrHGG84B1nHq6QHBAwhT000Pc8rg5fXnvGjGPI0cM7DDEIFr0SBft18nfMJ6kteg-J5F7uehUneEmoXBPscMC6poxS7-SR1QoyLH1yP9QMajwq0AMeOwDNCfdgVMcZFPb0RcL_.

CB Insights. 2018. “Blockchain Startups Absorbed 5X More Capital Via ICOs Than Equity Financings In 2017.” CB Insights. January 18, 2018. https://www.cbinsights.com/research/blockchain-vc-ico-funding/.

Chauhan, A., O. P. Malviya, M. Verma, and T. S. Mor. 2018. “Blockchain and Scalability.” In *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, 122–28. IEEE.

CoinMarketCap. n.d. “CoinMarketCap: Decision Token (HST).” CoinMarketCap. Accessed September 12, 2019. https://coinmarketcap.com/currencies/decision-token/.

Committee of Ministers. 2017. “Recommendation CM/Rec(2017)51 of the Committee of Ministers to Member States on Standards for E-Voting.” CM/Rec(2017)5. Council of Europe. https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680726f6f.

Council of Europe. Directorate General of Democracy and Political Affairs. 16, Feb 2011. “Guidelines on Transparency of E-Enabled Elections.” GGIS (2010) 5 fin. E. Council of Europe.

Crunchbase. n.d.a. “Follow My Vote, Inc.” Crunchbase. Accessed September 9, 2019. https://www.crunchbase.com/organization/follow-my-vote-inc#section-overview.

Crunchbase. n.d.b. “Voatz.” Crunchbase. Accessed September 10, 2019. https://www.crunchbase.com/organization/voatz#section-overview.

Crunchbase. n.d.c. “Horizon State.” Crunchbase. Accessed September 10, 2019. https://www.crunchbase.com/organization/horizon-state#section-funding-rounds.

Cucurull, Jordi, Adrià Rodríguez-Pérez, Tamara Finogina, and Jordi Puiggalí. 2019. “Blockchain-Based Internet Voting: Systems’ Compliance with International Standards.” In *Business Information Systems Workshops*, edited by Witold Abramowicz and Adrian Paschke, 300–312. Springer International Publishing.

Cuvelier, Édouard, Olivier Pereira, and Thomas Peters. 2013. “Election Verifiability or Ballot Privacy: Do We Need to Choose?” In *Computer Security – ESORICS 2013*, 481–98. Berlin, Heidelberg: Springer.

Dillman, Don A. 2007. Mail and Internet Surveys: The Tailored Design Method. John Wiley & Sons Inc.

Dogo, E. M., N.I. Nwulu, Olayemi M. Olaniyi, Clinton Aigbavboa and Thembinkosi Nkonyana. 2018. “Blockchain 3.0: Towards a Secure Ballotcoin Democracy through a Digitized Public Ledger in Developing Countries.” In *Conference: 2nd International Conference on Information and Communication Technology and Its Applications (ICTA 2018):* Federal University of Technology, Nigeria.

Dotson, Kyt. 2017. “Kaspersky Lab Unveils Secure Blockchain-Based Voting Platform - SiliconANGLE.” SiliconANGLE. November 13, 2017. https://siliconangle.com/2017/11/13/kaspersky-lab-unveils-secure-blockchain-based-voting-platform/.

Ernest, Adam Kaleb. 2014. “The Key To Unlocking The Black Box: Why The World Needs A Transparent Voting DAC.” FollowMyVote.

Fenton, Andrew. 2019. “Horizon State ‘Flat out with Demand’ from Secret New Clients | Micky.” Micky. July 1, 2019. https://micky.com.au/horizon-state-flat-out-with-demand-from-secret-new-clients/.

F.M.Mursi, Mona, Mona F. M. Mursi, Ghazy M. R. Assassa, Ahmed Abdelhafez, and Kareem M. Abo Samra. 2013. “On the Development of Electronic Voting: A Survey.” *International Journal of Computer Applications* 61 (16): 1–11.

Germann, Micha, and Uwe Serdült. 2017. “Internet Voting and Turnout: Evidence from Switzerland.” *Electoral Studies* 47 (June): 1–12.

Goggin, Stephen N., Michael D. Byrne, and Juan E. Gilbert. 2012. “Post-Election Auditing: Effects of Procedure and Ballot Type on Manual Counting Accuracy, Efficiency, and Auditor Satisfaction and Confidence.” *Election Law Journal: Rules, Politics, and Policy* 11 (1): 36–51.

Gritzalis, Dimitris A. 2012. *Secure Electronic Voting*. Springer Science & Business Media.

Hanifatunnisa, R., and B. Rahardjo. 2017. “Blockchain Based E-Voting Recording System Design.” In *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*, 1–6. IEEE.

Hjálmarsson, Friorik P., and Gunnlaugur K. Hreioarsson. 2018. “Blockchain-Based E-Voting System.” Edited by Mohammad Adnan Hamdaqa, Anton Már Egilsson, and Kristinn Steinar Kristinsson. Bachelor’s, Reykjavík University. https://skemman.is/bitstream/1946/31161/1/Research-Paper-BBEVS.pdf.

Hayes, Adam. 2019. “White Paper: What Everyone Should Know.” Investopedia. November 18, 2019. https://www.investopedia.com/terms/w/whitepaper.asp.

Hill, Richard. 2016. “E-Voting and the Law. Issues, Solutions, and a Challenging Question.” In *The International Conference on Electronic Voting: E-Vote-ID 2016*, 123–38.

Horizon State. 2017. “Horizon State - Decentralised Engagement and Decision Platform.” Horizon State. https://cryptorating.eu/whitepapers/Horizon-State/horizon_state_white_paper.pdf.

Jackson, Donovan. 2018. “Modifying Democracy with the Blockchain.” iStart. February 8, 2018. https://istart.com.au/feature-article/modifying-democracy-blockchain-secure-voting/.

Jonker, Hugo, Sjouke Mauw, and Jun Pang. 2013. "Privacy and verifiability in voting systems: Methods, developments and trends." *Computer Science Review* 10: 1-30.

Juels, Ari, Dario Catalano, and Markus Jakobsson. 2010. "Coercion-resistant electronic elections." In *Towards Trustworthy Elections*, 37-63. Springer, Berlin, Heidelberg.

Kendall, J. M. 2003. “Designing a Research Project: Randomised Controlled Trials and Their Principles.” Emergency Medicine Journal: EMJ 20 (2): 164–68.

Konzok, Ivo. 2020. “The Impact of Blockchain Technology on the Trustworthiness of Online Voting Systems – An Exploration of Blockchain Technology”. NOVA School of Business and Economics. Lisbon.

Krimmer, Robert, David Duenas-Cid, Iuliia Krivonosova, Priit Vinkel, and Arne Koitmae. 2018. “How Much Does an E-Vote Cost? Cost Comparison per Vote in Multichannel Elections in Estonia.” In *International Joint Conference on Electronic Voting*: 117–31. Cham: Springer.

Krivonosova, Iullia, Serrano, R. Antnoio, Duenas-Cid, David and Krimmer, Robert. 2019. “How increasing use of Internet voting impacts the Estonian election management.” In *Fourth International Joint Conference on Electronic Voting E-Vote-ID 2019.* 1-4. Taltech Press.

Krivoruchko, Taisya. 2007. "Robust coercion-resistant registration for remote e-voting." In *Proceedings of the IAVoSS Workshop on Trustworthy Elections (WOTE 2007)*.

Lambrinoudakis, Costas, Dimitris Gritzalis, Vassilis Tsoumas, Maria Karyda, and Spyros Ikonomopoulos. 2003. “Secure Electronic Voting: The Current Landscape.” In *Secure Electronic Voting*, edited by Dimitris A. Gritzalis, 101–22. Springer, Boston, MA.

Lewis, Rebecca, John McPartland, and Rajeev Ranjan. 2017. “Blockchain and Financial Market Innovation.” *Economic Perspectives* 41 (7): 1–17.

Lowe, Kevin, Christine Tennent, John Guenther, Neil Harrison,Cathie Burgess, C., Moodie, N. and Vass, G., 2019. “Aboriginal Voices: An overview of the methodology applied in the systematic review of recent research across ten key areas of Australian Indigenous education.” *The Australian Educational Researcher* 46(2). 213-229. doi: 10.1007/s13384-019-00307-5.

Mc Galey, Margaret, and J. Paul Gibson. 2003. “Electronic Voting: A Safety Critical System.” Final Year Project Report. NUI Maynooth Department of Computer Science.

Mcknight, D. Harrison, Michelle Carter, Jason B. Thatcher, and Paul Clay. 2011. „Trust in a specific technology: An investigation in its components and measures“, *ACM Transactions on Management Information Systems* 2(2), 1–12. https://doi.org/10.1145/1985347. 1985353.

Medici. n.d. “Companies — Medici Ventures INC.” Medici Ventures INC. Accessed September 12, 2019. https://www.mediciventures.com/companies.

Moore, Larry and Nimit Sawhney. 2019. “Under the Hood: The West Virginia Mobile Voting Pilot.” Voatz. https://blog.voatz.com/wp-content/uploads/2019/02/West-Virginia-Mobile-Voting-White-Paper-NASS-Submission.pdf.

Moynihan, Donald P. 2004. “Building Secure Elections: E-Voting, Security, and Systems Theory.” *Public Administration Review* 64 (5): 515–28.

Nakamoto, Satoshi. 2008. “Bitcoin: A Peer-to-Peer Electronic Cash System.” https://bitcoin.org/bitcoin.pdf.

Paul, Nathanael, David Evans, Avi Rubin, and Dan Wallach. 2003."Authentication for remote voting." In *Workshop on Human-Computer Interaction and Security Systems*. 2003.

Pitchbook. n.d. “Votem Company Profile: Valuation & Investors.” Pitchbook. Accessed September 9, 2019. https://pitchbook.com/profiles/company/136806-04.

Polys. 2017. “Polys - Online Voting Systems.” Polys. https://polys.me/assets/docs/Polys_whitepaper.pdf.

Reuters. 2018. “Blockchain explained.” Accessed September 26. http://graphics.reuters.com/TECHNOLOGYBLOCKCHAIN/010070P11GN/index.html.

Russell, Martin, and Ionel Zamfir. 2018. “Digital Technology in Elections - Efficiency versus Credibility?” European Parliamentary Research Service. Accessed December 2019. http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/625178/EPRS_BRI(2018)625178_EN.pdf.

Sál, Karel. 2015. “Remote Internet Voting and Increase of Voter Turnout: Happy Coincidence or Fact? The Case of Estonia.” *Masaryk University Journal of Law and Technology* 9 (2): 15–32.

Seedorf, Sebastian. 2016. “Germany: The Public Nature of Elections and Its Consequences for E-Voting.” In *E-Voting Case Law*, edited by Ardita Driza Maurer and Jordi Barrat, 23–44. Routledge.

Spycher, Oliver, Melanie Volkamer, and Reto Koenig. 2011. “Transparency and technical measures to establish trust in norwegian internet voting.” In *International Conference on E-Voting and Identity: VoteID11*, 19-35. Berlin: Springer.

Susskind, Jane. 1, Dez 2017. “Decrypting Democracy: Incentivizing Blockchain Voting Technolog Y for an Improved Election System.” *San Diego Law Review* 54 (4): 785–827.

Tosh, Deepak K., Sachin Shetty, Xueping Liang, Charles A. Kamhoua, Kevin A. Kwiat, and Laurent Njilla. 2017. “Security Implications of Blockchain Cloud with Analysis of Block Withholding Attack.” In *Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, 458–67. IEEE Press.

Valenty, Linda O., and James C. Brent. 2000. “Online Voting: Calculating Risks and Benefits to the Community and the Individual.” In *The Internet Upheaval: Raising Questions, Seeking Answers in Communications Policy*, edited by Ingo Vogelsang and Benjamin M. Compaine, 99–126. MIT Press.

Varghese, Sam. 2017. “Australian Start-up Testing New Online Voting System.” IT Wire. March 7, 2017. https://www.itwire.com/government-tech-policy/77149-australian-start-up-testing-new-online-voting-system.html.

Vassil, Kristjan, Mihkel Solvak, Priit Vinkel, Alexander H. Trechsel, and R. Michael Alvarez. 2016. “The Diffusion of Internet Voting. Usage Patterns of Internet Voting in Estonia between 2005 and 2015.” *Government Information Quarterly* 33 (3): 453–59.

Voatz. 2019a. “West Virginia Secretary of State announces UOCAVA mobile voting pilot for 2018 primary elections.” Accessed December 7. https://blog.voatz.com/?p=39.

Voatz. 2019b. “Voatz collaborates with WGBH’s national center for accessible media to make mobile voting accessible for voters with disabilities and citizens residing overseas.” Accessed December 7. https://blog.voatz.com/?p=1117.

Volkamer, Melanie, Oliver Spycher, and Eric Dubuis. 2011. "Measures to establish trust in internet voting." In *Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance*, 1-10. ACM.

Votem. 2017a. “Case Study - Rock and Roll Hall of Fame.” Votem. 2017. http://www.votem.com/wp-content/uploads/2017/04/RRHoF-Case-Study.pdf.

Votem. 2017b. “Votem - Voting for a Mobile World: Introducing the VAST Token.” Votem. https://www.votem.io/assets/docs/wp.pdf.

Vysna, Nina. 2020. “The Impact of Blockchain Technology on the Trustworthiness of Online Voting Systems – Elections and Trust”. NOVA School of Business and Economics. Lisbon.

Willemson, Jan. 2017. “Bits or Paper: Which Should Get to Carry Your Vote?” In *Electronic Voting - Second International Joint Conference, E-Vote-ID 2017 Bregenz, Austria, October 24–27, 2017 Proceedings*, edited by Robert Krimmer, Melanie Volkamer, Binder Nadja Braun, Norbert Kersting, Olivier Pereira, and Carsten Schürmann, 292–305. E-Vote-ID. Springer.

Wolf, Peter, Rushdi Nackerdien, and Domenico Tuccinardi. Dez, 2011. “Introducing Electronic Voting: Essential Considerations.” International Institute for Democracy and Electoral Assistance. https://www.idea.int/sites/default/files/publications/introducing-electronic-voting.pdf.

Wu, Shuang. 2018. “Evaluation and Improvement of Two Blockchain Based E-Voting System: Agora and Proof of Vote.” Edited by David Galindo. University of Birmingham. http://www.dgalindo.es/mscprojects/shuang.pdf.

6. Appendices

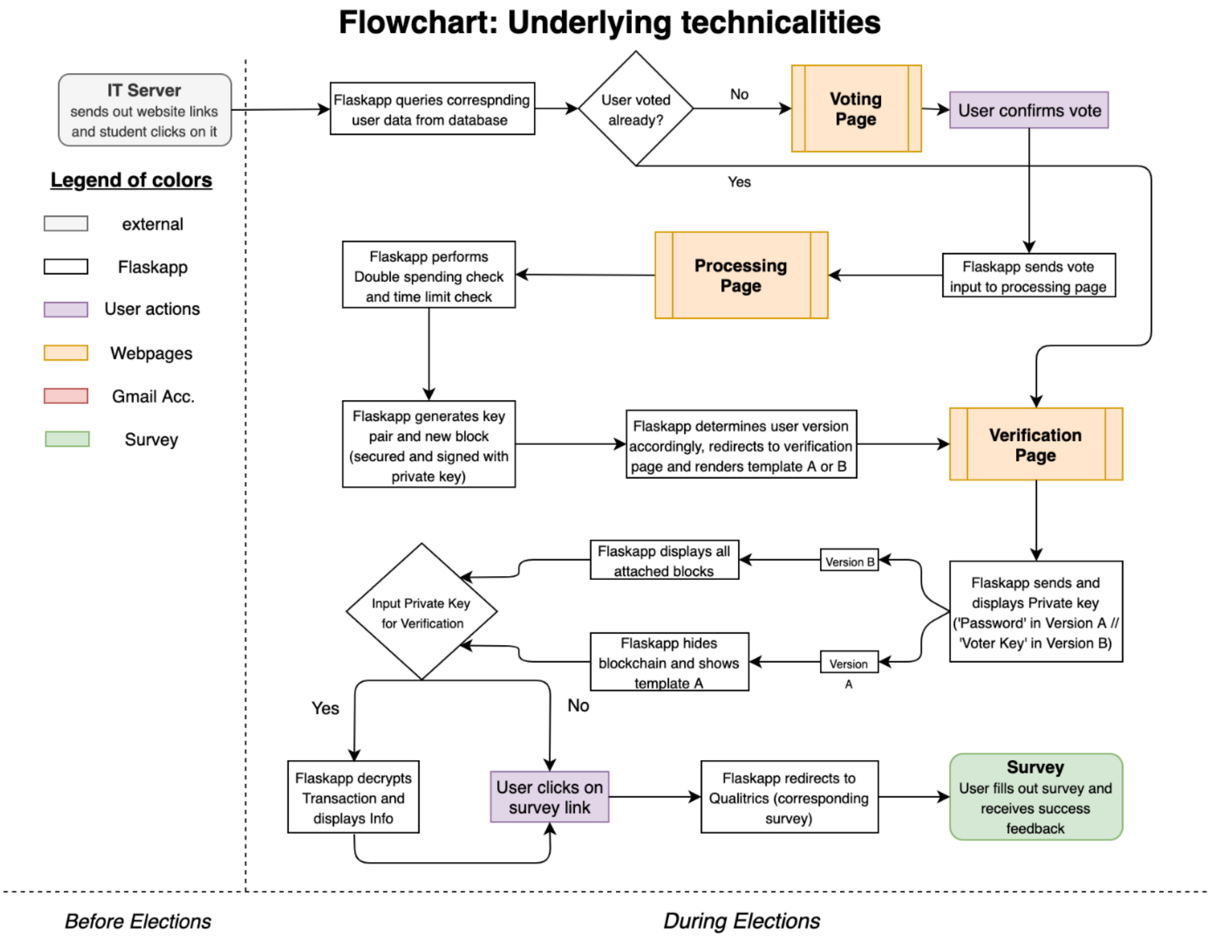
Appendix 1: Comparison of seven existing blockchain-based online voting systems

Name	Founded	Funding	Real Life Experiments	Blockchain Technology	Encryption Technology	Unique Features	Business Model
Follow-MyVote[1]	2012 USA	$71,400 and support with providing office space.[2]	Nothing published up until the end of 2019.	Public version of the BitShares blockchain.	Elliptic Curve Cryptography for user identification. No encryption for the votes.	Provides long-term privacy because no encryption for the votes is used which could be decrypted by quantum computers in the future. First Voting DAC of the industry.	Service requires the purchase of FollowMyVote tokens called VOTES. Their value is estimated to increase over time since there is just a limited amount and they will get destroyed after their use. Token holders, such as FollowMyVote itself and investors benefit from the increase in value.
SecureVote[3,4]	2017 AUS	$500,000 of early-stage funding.	Implemented a governance structure within the token-based investment platform Swarm. Ran a 24 hours stress test, processing 1.5 billion votes in that time.	Combination of a public version of the Ethereum blockchain and an Inter Planetary File System (IPFS) in order to store the votes.	Ballot encryption is handled by their own anonymization algorithm called 'Copperfield'. No further information published.	SecureVote developed their own algorithm called 'Copperfield' to provide secret ballots. It's also possible to obtain a receipt for a different vote to solve the coercion problem.	SecureVote is not offering their services for everyone but individual clients. They are especially targeting to optimize governance structures within cryptocurrencies and tokens by enabling token-holders to vote.
Votem[5]	2014 USA	Series A Funding round of $ 1.2 million invested by Medici Ventures.[6]	Multiple successfully hosted elections including general state elections, labour union polls and the currently biggest blockchain powered election with 1.8 million counted votes for the Rock and Roll Hall of Fame.[7]	Currently using a Tendermint framework blockchain. In the future they are targeting a hybrid of a public version of the Ethereum blockchain and a private blockchain.	Combination of ElGamal encryption and mixnet technologies.	Votem offers a fully customizable product which depends on the needs of the customer. They can pick any combination of features for their specific election. The cost structure adjusts accordingly which also enables smaller, less complex elections to use the application for reasonable costs.	Votem introduced the VAST token which is required to use the service. Tokens can be used for multiple elections but not simultaneously. The most basic election requires just one token. The more features the voting authority wants to implement and the more complex an election gets (voter authentication etc.) the more tokens have to be purchased to support it.
Polys[8,9]	2017 RUS	No funding published. Project powered by the Kaspersky Lab.	Several successfully supported elections in cooperation with universities, conferences and the government. The biggest use-case counted more than 82,000 votes.	Private version of the Ethereum blockchain.	ElGamal encryption for the votes.	Up to 100 voters, Polys can be used free of charge. The website provides previews of the election on different devices and the possibility to choose between several voting methods and voter access points.	The project got created by Kaspersky Lab. They offer a free plan called 'Basic', which allows to create an unlimited amount of elections and polls with 100 votes per election. The commercial Pro-Version enables more features such as rebranding the service and white-labeling. Prices vary based on request.

Name	Founded	Funding	Real Life Experiments	Blockchain Technology	Encryption Technology	Unique Features	Business Model
Voatz[10]	2014 USA	$ 9.3 million while a majority of the funding was raised during a Series A funding round in June 2019 led by Medici Ventures.[11]	Within the municipal public elections in Denver 2019, over 4,000 international voters were allowed to vote with the Voatz mobile app. 24 counties of West Virginia used Voatz for Midterm General Elections in 2018.	The application utilizes the Hyperledger blockchain software. No more specific information provided by Voatz.	The whitepaper refers to encryption technologies several times but does not mention any specific algorithms.	Voatz is leveraging biometric information (fingerprints, face id), provided by modern smartphones for the authentication process.	The mobile application is just available by invitation of Voatz's election organizer and not for the general public. The app primary aims for the transformation of public elections while making a profit out of it. Voatz did not publish any source code and does not provide information about prices without requesting an offer for a specific election and providing corresponding information.
Agora[12,13]	2015 SUI	Agora has not published any funding yet but promoted the ICO of its VOTE token in mid 2019 which could help them raise up to $20 million.	First support ever of a national government election by blockchain technology. Parts of the Presidential Elections 2018 in Sierra Leone were registered and processed by the Agora system.[14]	Hybrid of private version of blockchain and the public Bitcoin blockchain.	Combination of ElGamal encryption and mixnet technologies.	Agora developed a five-layer model for their application with innovative combinations of the public Bitcoin blockchain and their self-created permission blockchain called 'Skipchain' which allows verifying blocks and transactions without the need of a complete copy of the blockchain.	Based on a formula containing average blockchain network fees and the election population, a dollar amount of VOTE tokens is purchased and form a bonus pool. This pool will be distributed between permissioned and permissionless blockchain nodes (which are VOTE token holders) after the election. These costs represent Agora's profit and have to be paid by the customers.
Horizon State[15,16]	2017 NZ	Raised $ 1.1 million by the ICO of Horizon State's coin called 'Decision Token'.[1]	They supported a leadership election with 4,500 members of the Opportunities party New Zealand and an election of the Southern Australian government with 1,450 participants.	Public version of the Ethereum blockchain.	The whitepaper does not provide any sort of encryption methods in order to anonymize ballots.	The idea of Horizon State is more focused on creating a decision-making ecosystem. While doing so, they work on many 'secondary' applications which customers can use next to voting.	Horizon State aims to create a platform where customers can use their service by paying with Decision Tokens. These can be purchased by Horizon State or over a marketplace they provide. The supply of tokens will decrease over time and a small percentage of the costs for the elections will be donated to governmental and non-profit projects by Horizon State.

[1] (Ernest, 2014) [2] (Crunchbase n.d.a) [3] (Varghese, 2017) [4] (Jackson, 2018) [5] (Votem, 2017b) [6] (Pitchbook, n.d.) [7] (Votem, 2017a) [8] (Polys, 2017) [9] (Dotson, 2017)
[10] (Moore and Sawhney, 2019) [11] (Crunchbase, n.d.b) [12] (Agora, 2015) [13] (Wu, 2018) [14] (Agora, 2018) [15] (Fenton, 2019) [16] (Horizon State, 2017) [17] (Crunchbase, n.d.c)

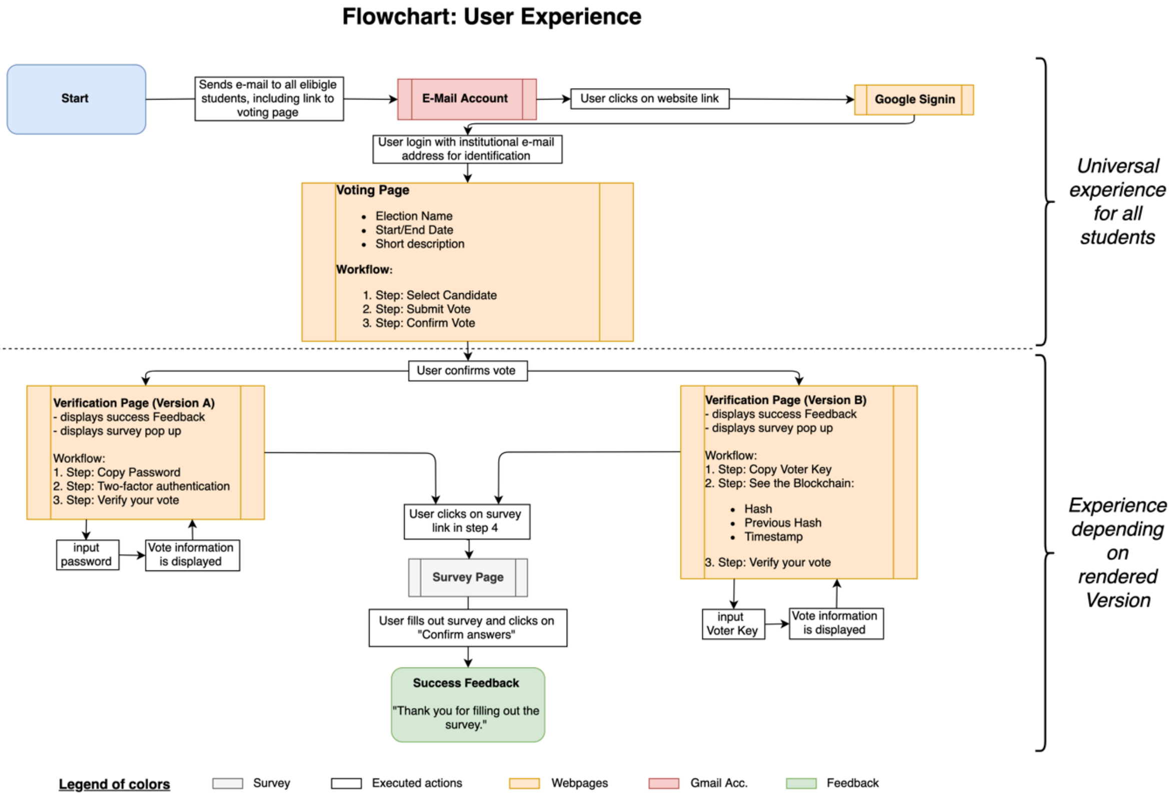
Appendix 2: Backend flowchart of our blockchain-based online voting system


Flowchart: Underlying technicalities
IT Server
sends out website links and student clicks on it
Legend of colors
external
Flaskapp
User actions
Webpages
Gmail Acc.
Survey
Flaskapp queries correspnding user data from database
User voted already?
No
Yes
Voting Page
User confirms vote
Flaskapp sends vote input to processing page
Processing Page
Flaskapp performs Double spending check and time limit check
Flaskapp generates key pair and new block (secured and signed with private key)
Flaskapp determines user version accordingly, redirects to verification page and renders template A or B
Verification Page
Flaskapp sends and displays Private key ('Password' in Version A // 'Voter Key' in Version B)
Version B
Version A
Flaskapp displays all attached blocks
Flaskapp hides blockchain and shows template A
Input Private Key for Verification
Yes
No
Flaskapp decrypts Transaction and displays Info
User clicks on survey link
Flaskapp redirects to Qualitrics (corresponding survey)
Survey
User fills out survey and receives success feedback
Before Elections
During Elections

Appendix 3: Github URL for the source code of Votechain

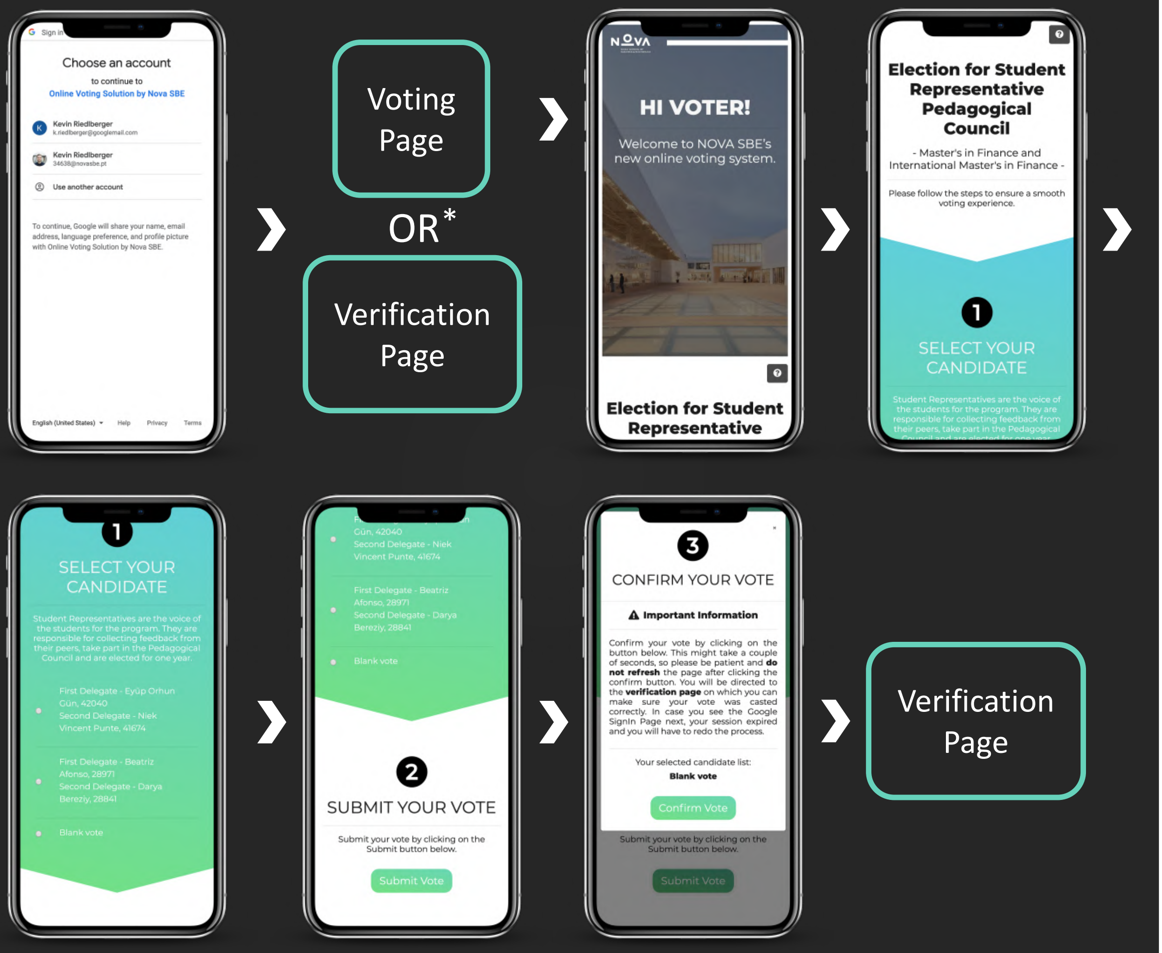
https://github.com/K-Rdlbrgr/master_thesis

Appendix 4: User Experience Flowchart of Votechain


Flowchart: User Experience
Start
Sends e-mail to all elibigle students, including link to voting page
E-Mail Account
User clicks on website link
Google Signin
User login with institutional e-mail address for identification
Voting Page
• Election Name
• Start/End Date
• Short description
Workflow:
1. Step: Select Candidate
2. Step: Submit Vote
3. Step: Confirm Vote
Universal experience for all students
User confirms vote
Verification Page (Version A)
- displays success Feedback
- displays survey pop up
Workflow:
1. Step: Copy Password
2. Step: Two-factor authentication
3. Step: Verify your vote
input password
Vote information is displayed
User clicks on survey link in step 4
Survey Page
User fills out survey and clicks on "Confirm answers"
Success Feedback
"Thank you for filling out the survey."
Verification Page (Version B)
- displays success Feedback
- displays survey pop up
Workflow:
1. Step: Copy Voter Key
2. Step: See the Blockchain:
• Hash
• Previous Hash
• Timestamp
3. Step: Verify your vote
input Voter Key
Vote information is displayed
Experience depending on rendered Version
Legend of colors
Survey
Executed actions
Webpages
Gmail Acc.
Feedback

Appendix 5: Votechain's first stage of the voting procedure

Google Sign In + Voting Page



Sign in

Choose an account

to continue to

Online Voting Solution by Nova SBE

Kevin Riedlberger
k.riedlberger@googlemail.com

Kevin Riedlberger
34638@novasbe.pt

Use another account

To continue, Google will share your name, email address, language preference, and profile picture with Online Voting Solution by Nova SBE.

English (United States) ▾ Help Privacy Terms

❯

Voting Page

OR*

Verification Page

❯

NOVA

HI VOTER!

Welcome to NOVA SBE's new online voting system.

Election for Student Representative

❯

Election for Student Representative Pedagogical Council

- Master's in Finance and International Master's in Finance -

Please follow the steps to ensure a smooth voting experience.

1

SELECT YOUR CANDIDATE

Student Representatives are the voice of the students for the program. They are responsible for collecting feedback from their peers, take part in the Pedagogical Council and are elected for one year.

❯

1

SELECT YOUR CANDIDATE

Student Representatives are the voice of the students for the program. They are responsible for collecting feedback from their peers, take part in the Pedagogical Council and are elected for one year.

○ First Delegate - Eyüp Orhun Gün, 42040
Second Delegate - Niek Vincent Punte, 41674

○ First Delegate - Beatriz Afonso, 28971
Second Delegate - Darya Bereziy, 28841

○ Blank vote

❯

2

SUBMIT YOUR VOTE

Submit your vote by clicking on the Submit button below.

Submit Vote

❯

3

CONFIRM YOUR VOTE

Important Information

Confirm your vote by clicking on the button below. This might take a couple of seconds, so please be patient and **do not refresh** the page after clicking the confirm button. You will be directed to the **verification page** on which you can make sure your vote was casted correctly. In case you see the Google SignIn Page next, your session expired and you will have to redo the process.

Your selected candidate list:

Blank vote

Confirm Vote

Submit your vote by clicking on the Submit button below.

Submit Vote

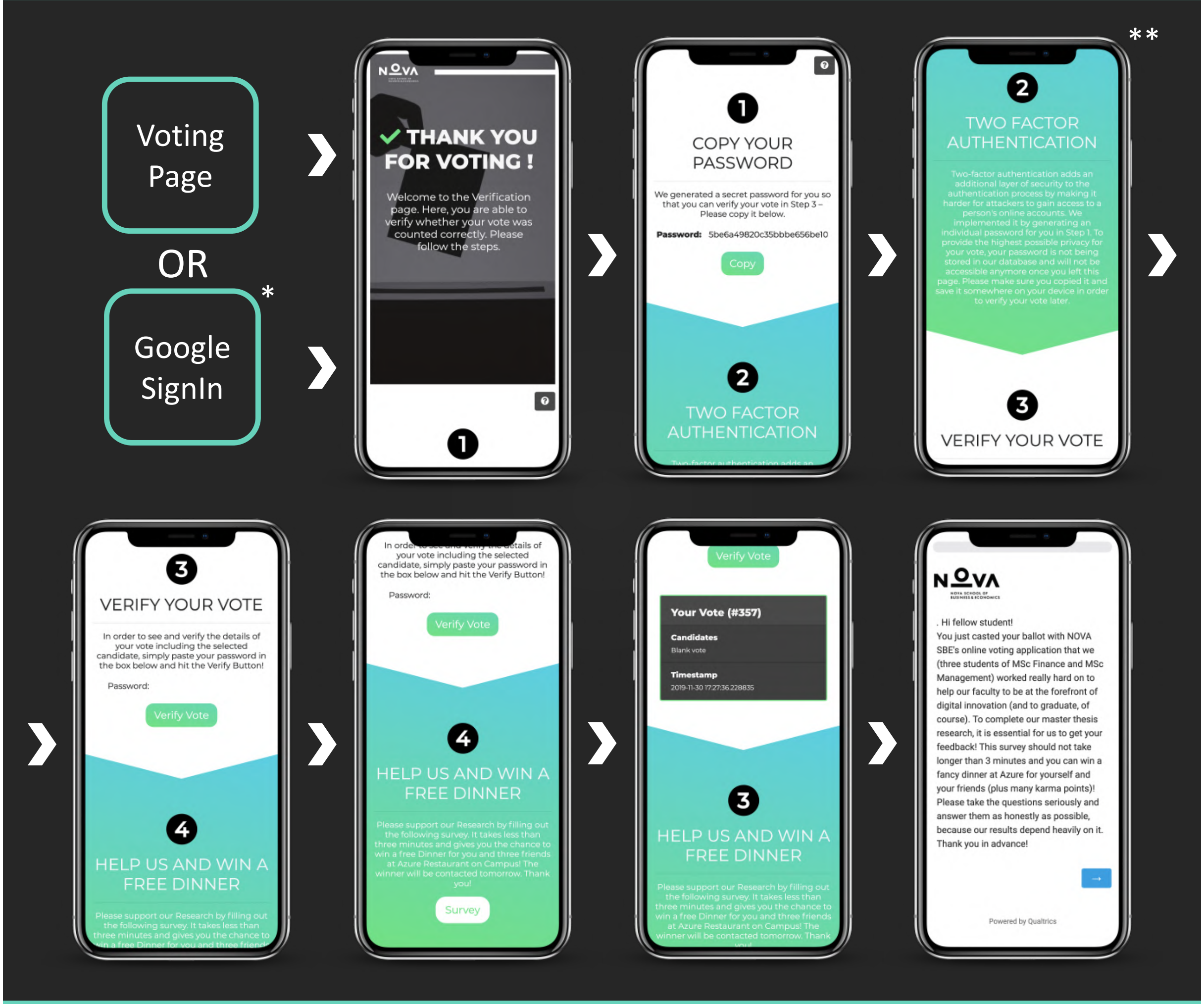
❯

Verification Page

*Where the user will be directed to after the sign in with Google depends on his voting status. If the user voted already, he or she will get directed to the verification page. In case the user has not casted a vote yet, he or she will be directed to the voting page.

Appendix 6: Votechain's second stage of the voting procedure (using version A)

Verification Page + Survey : Version A



NOVA

✓ THANK YOU FOR VOTING !

Welcome to the Verification page. Here, you are able to verify whether your vote was counted correctly. Please follow the steps.

1

1

COPY YOUR PASSWORD

We generated a secret password for you so that you can verify your vote in Step 3 – Please copy it below.

Password: 5be6a49820c35bbbe656be10

Copy

2

TWO FACTOR AUTHENTICATION

2

TWO FACTOR AUTHENTICATION

Two-factor authentication adds an additional layer of security to the authentication process by making it harder for attackers to gain access to a person's online accounts. We implemented it by generating an individual password for you in Step 1. To provide the highest possible privacy for your vote, your password is not being stored in our database and will not be accessible anymore once you left this page. Please make sure you copied it and save it somewhere on your device in order to verify your vote later.

3

VERIFY YOUR VOTE

3

VERIFY YOUR VOTE

In order to see and verify the details of your vote including the selected candidate, simply paste your password in the box below and hit the Verify Button!

Password:

Verify Vote

4

HELP US AND WIN A FREE DINNER

Please support our Research by filling out the following survey. It takes less than three minutes and gives you the chance to win a free Dinner for you and three friends

In order to see and verify the details of your vote including the selected candidate, simply paste your password in the box below and hit the Verify Button!

Password:

Verify Vote

4

HELP US AND WIN A FREE DINNER

Please support our Research by filling out the following survey. It takes less than three minutes and gives you the chance to win a free Dinner for you and three friends at Azure Restaurant on Campus! The winner will be contacted tomorrow. Thank you!

Survey

Verify Vote

Your Vote (#357)

Candidates
Blank vote

Timestamp
2019-11-30 17:27:36.228835

3

HELP US AND WIN A FREE DINNER

Please support our Research by filling out the following survey. It takes less than three minutes and gives you the chance to win a free Dinner for you and three friends at Azure Restaurant on Campus! The winner will be contacted tomorrow. Thank you!

NOVA
NOVA SCHOOL OF BUSINESS & ECONOMICS

. Hi fellow student!
You just casted your ballot with NOVA SBE's online voting application that we (three students of MSc Finance and MSc Management) worked really hard on to help our faculty to be at the forefront of digital innovation (and to graduate, of course). To complete our master thesis research, it is essential for us to get your feedback! This survey should not take longer than 3 minutes and you can win a fancy dinner at Azure for yourself and your friends (plus many karma points)! Please take the questions seriously and answer them as honestly as possible, because our results depend heavily on it. Thank you in advance!

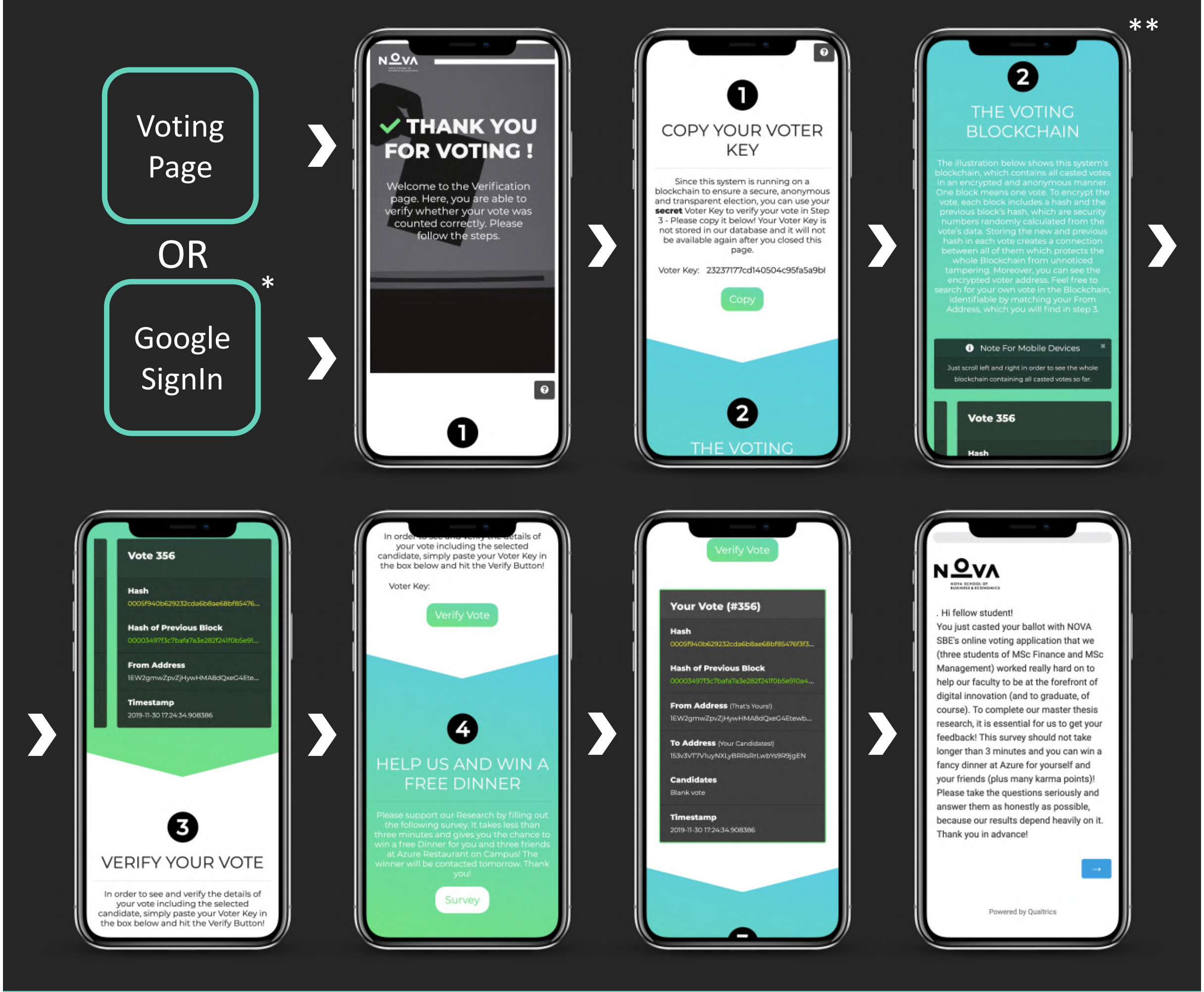
→

Powered by Qualtrics

*Users who already voted and sign in with Google again, get directed straight to the verification page. In this case the verification page does neither contain the 'thank you for voting' banner, nor provides the password (the page in this case starts at **). Users are still able to verify their vote and participate in the survey.

Appendix 7: Votechain's second stage of the voting procedure (using version B)

Verification Page + Survey : Version B



✓ THANK YOU FOR VOTING !

Welcome to the Verification page. Here, you are able to verify whether your vote was counted correctly. Please follow the steps.

1 COPY YOUR VOTER KEY

Since this system is running on a blockchain to ensure a secure, anonymous and transparent election, you can use your **secret** Voter Key to verify your vote in Step 3 - Please copy it below! Your Voter Key is not stored in our database and it will not be available again after you closed this page.

Voter Key: 23237177cd140504c95fa5a9b!

Copy

2 THE VOTING BLOCKCHAIN

The illustration below shows this system's blockchain, which contains all casted votes in an encrypted and anonymous manner. One block means one vote. To encrypt the vote, each block includes a hash and the previous block's hash, which are security numbers randomly calculated from the vote's data. Storing the new and previous hash in each vote creates a connection between all of them which protects the whole Blockchain from unnoticed tampering. Moreover, you can see the encrypted voter address. Feel free to search for your own vote in the Blockchain, identifiable by matching your From Address, which you will find in step 3.

Note For Mobile Devices

Just scroll left and right in order to see the whole blockchain containing all casted votes so far.

Vote 356

Hash
0005f940b629232cda6b8ae68bf85476...

Hash of Previous Block
00003497f3c7bafa7a3e282f241f0b5e91...

From Address
1EW2gmwZpvZjHywHMA8dQxeG4Ete...

Timestamp
2019-11-30 17:24:34.908386

3 VERIFY YOUR VOTE

In order to see and verify the details of your vote including the selected candidate, simply paste your Voter Key in the box below and hit the Verify Button!

Voter Key:

Verify Vote

4 HELP US AND WIN A FREE DINNER

Please support our Research by filling out the following survey. It takes less than three minutes and gives you the chance to win a free Dinner for you and three friends at Azure Restaurant on Campus! The winner will be contacted tomorrow. Thank you!

Survey

Your Vote (#356)

Hash
0005f940b629232cda6b8ae68bf85476f3f3...

Hash of Previous Block
00003497f3c7bafa7a3e282f241f0b5e910a4...

From Address (That's Yours!)
1EW2gmwZpvZjHywHMA8dQxeG4Etewb...

To Address (Your Candidates!)
153v3VT7V1uyNXLyBRRsRrLwbYs9R9jgEN

Candidates
Blank vote

Timestamp
2019-11-30 17:24:34.908386

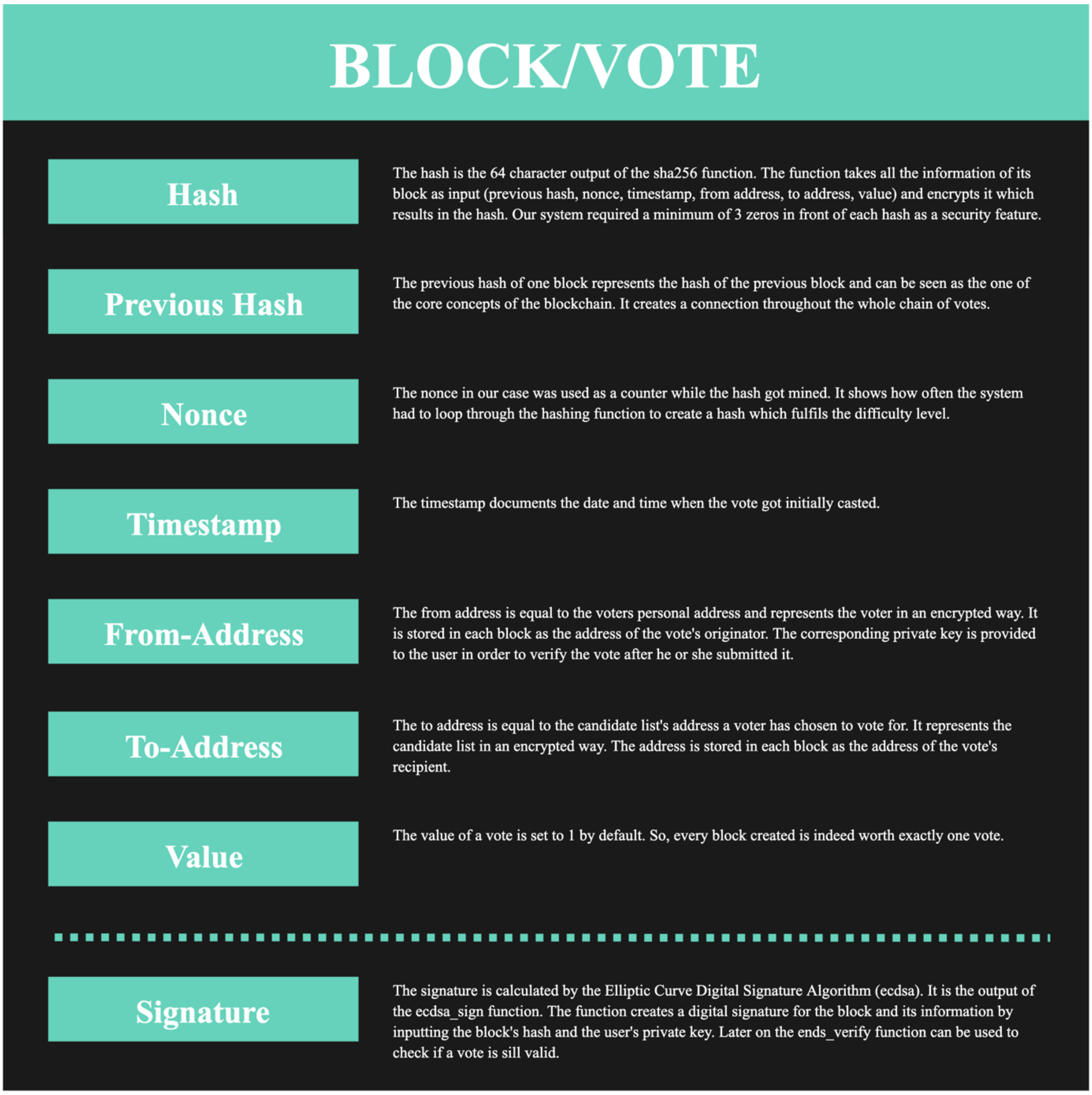
NOVA SCHOOL OF BUSINESS & ECONOMICS

. Hi fellow student!
You just casted your ballot with NOVA SBE's online voting application that we (three students of MSc Finance and MSc Management) worked really hard on to help our faculty to be at the forefront of digital innovation (and to graduate, of course). To complete our master thesis research, it is essential for us to get your feedback! This survey should not take longer than 3 minutes and you can win a fancy dinner at Azure for yourself and your friends (plus many karma points)! Please take the questions seriously and answer them as honestly as possible, because our results depend heavily on it. Thank you in advance!

Powered by Qualtrics

*Users who already voted and sign in with Google again, get directed straight to the verification page. In this case the verification page does neither contain the 'thank you for voting' banner, nor provides the password (the page in this case starts at **). Users are still able to verify their vote and participate in the survey.

Appendix 8: Information about the properties of one block/vote of Votechain



BLOCK/VOTE

Hash

The hash is the 64 character output of the sha256 function. The function takes all the information of its block as input (previous hash, nonce, timestamp, from address, to address, value) and encrypts it which results in the hash. Our system required a minimum of 3 zeros in front of each hash as a security feature.

Previous Hash

The previous hash of one block represents the hash of the previous block and can be seen as the one of the core concepts of the blockchain. It creates a connection throughout the whole chain of votes.

Nonce

The nonce in our case was used as a counter while the hash got mined. It shows how often the system had to loop through the hashing function to create a hash which fulfils the difficulty level.

Timestamp

The timestamp documents the date and time when the vote got initially casted.

From-Address

The from address is equal to the voters personal address and represents the voter in an encrypted way. It is stored in each block as the address of the vote's originator. The corresponding private key is provided to the user in order to verify the vote after he or she submitted it.

To-Address

The to address is equal to the candidate list's address a voter has chosen to vote for. It represents the candidate list in an encrypted way. The address is stored in each block as the address of the vote's recipient.

Value

The value of a vote is set to 1 by default. So, every block created is indeed worth exactly one vote.

Signature

The signature is calculated by the Elliptic Curve Digital Signature Algorithm (ecdsa). It is the output of the ecdsa_sign function. The function creates a digital signature for the block and its information by inputting the block's hash and the user's private key. Later on the ends_verify function can be used to check if a vote is sill valid.

Appendix 9: Survey questions

Note: Answers to questions 1-25: Strongly agree; Agree; Somewhat agree; Neither agree nor disagree; Somewhat disagree; Disagree; Strongly disagree

Block 1 – Trust in specific technology construct:
<u>Reliability sub-construct items:</u>
Q1. NOVA's voting application is a very reliable piece of software.
Q2. NOVA's voting application does not fail me.
Q3. NOVA's voting application is extremely dependable.
Q4. NOVA's voting application does not malfunction for me.
<u>Functionality sub-construct items:</u>
Q5. NOVA's voting application has the functionality I need.
Q6. NOVA's voting application has the features required for casting a vote.

Q7. NOVA's voting application has the ability to do what I want it to do.
Helpfulness sub-construct items:
Q8. NOVA's voting application supplies my need for help through a help function.
Q9. NOVA's voting application provides competent guidance (as needed) through a help function.
Q10. NOVA's voting application provides very sensible and effective advice, if needed.

Block 2 – Trust in general technology construct:
Faith in general technology sub-construct items:
Q11. I believe that most technologies are effective at what they are designed to do.
Q12. A large majority of technologies are excellent.
Q13. Most technologies have the features needed for their domain.
Q14. I think most technologies enable me to do what I need to do.
Trusting Stance towards general technology sub-construct items:
Q15. My typical approach is to trust new technologies until they prove to me that I shouldn't trust them.
Q16. I usually trust a technology until it gives me a reason not to trust it.
Q17. I generally give a technology the benefit of the doubt when I first use it.

Block 3 – Institution-based trust:
Situational Normality sub-construct items:
Q18. I am totally comfortable working with online elections systems.
Q19. I feel very good about how things go when I use online elections systems.
Q20. I always feel confident that the right things will happen when I use online elections systems.
Q21. It appears that things will be fine when I utilize online elections systems.
Structural Assurance sub-construct items:
Q22. I feel okay using online elections systems because they are backed by vendor protections.
Q23. Product guarantees make it feel all right to use online elections systems.
Q24. Favorable-to-consumer legal structures help me feel safe working with online elections systems.
Q25. Having the backing of legal statutes and processes makes me feel secure in using online elections systems.

Block4 – Demographic and other questions:
Q26. What is your nationality?
Q27. What is your age?
Q28. What is your gender?
Q29. What is your ethnicity?
Q30. What program are you enrolled in?
Q31. Please provide your email below so we can contact you in case you win the lottery:
Q32. Would you potentially like to participate in a focus group study or do you want to learn more about project?

Appendix 10: Transcription of the focus group

Researcher 1: Welcome guys. Thanks for your time. We appreciate it a lot. So, this is going to be a 45min discussion. We are very interested in your opinion and your feedback in the voting which took place two weeks ago. We designed the whole system and it's very important to us. We really appreciate your feedback on this, so we can include this in our thesis as well. So let's go through some information which we have to go through so everybody is informed. So, just that you know, this whole thing is going to be anonymous. So none of your names will be anywhere and we will not track anything you said and connect it to your names. Also the tape if you're all okay with this, we would record this transcript, so we know what each of you said and then the tape will be delete. So, there's no voice of you or speech of you anywhere. Also if we include some options or something what you said, this will also be anonymous. So feel free to mention your real opinion, since you don't need to be afraid to be mentioned anywhere. So just some rules, so that we will have a smooth discussion. I will ask some questions about your experience with the system and then it would be really nice if everybody can mention their opinions.It would be nice if everybody could wait until the person stopped talking, so that we will not have interruptions. There is no right or wrong answers. It's all up to you. It's fully okay and we would even like to see if somebody has a totally different opinion than somebody else. Please feel free to refer to something others said. Somebody tells an opinion and you don't agree at all, so feel free to state this. Feel also free to state rally what you think although the rest of the group thinks differently. That's really appreciated. I think we went through all of the instructions. Any questions or concerns with that? Everyone feels comfortable with the situation? Great. Alright. I'm just gonna start by introducing myself or us and then I would be very happy if you state your name, nationality, degree as a small start up. Then like I said we will go through some questions if you even remember your experience from two weeks ago.

I'm Ivo, Master of Management student, that's Nine and Kevin, Master of Finance students and Andrew our professor who is supervising our master thesis.We teamed up for the master thesis and in the course of our master thesis we built this voting system and ran an experience two weeks ago. We were happy and obliged of the school that they actually allowed us to ru this experience. May you can start with saying one sentence about yourself.

Subject 1: My name is Subject 1 and I'm also a Master of Management student.

Subject 2: I'm Subject 2 and I'm in my second year of my Bachelors of Economics.

Subject 3: I'm Subject 3. Masters in Finance from Austria.

Subject 4: I'm Subject 4. Also Masters of Finance student and I'm from Austria as well.

Subject 5: I'm Subject 5. Also Masters of Finance student and also from Austria.

Subject 6: I'm Subject 6, Master's in Finance and I'm Portuguese.

Subject 7: I'm Subject 7. First year of Master in Finance and from Italy.

Researcher 1: Alright, perfect. Pretty diverse group with a slight edge to Austria.So let's have a look at the application again in order to refresh your memory on how the voting looked like. So you should have got to a page like this. Then there was your degree and your election displayed. Then you selected your candidate and voted. Then you were redirected to the second webpage which looked something like this. Now comes the most relevant part. You were directed to some blockchain picture like this. Does everyone remember this?

Everyone agreed

Perfect. So you saw, hopefully you got this already at this moment, we will figure out soon, but you should have been able to see this whole blockchain. So each of those blocks was one vote and you should have been able to transparently see in fact the whole election in an encrypted way. Then you were directed to this step where you were able to verify your own vote. Finally, you were coming to the survey. This is just an introduction, so everyone knows what we are talking about. I would jump in with the first question.

Question 1*:* Did you have any experience before with online voting systems. What's your general attitude or relationship with online voting systems. It's also fine if you never actually thought about this but what's your general attitude? Does anybody want to share any thoughts on this?

Subject 4: So I guess it would allow more people to actually vote. For example, if you implement it as a national wide election and implement an online system I would think it would encourage people to vote. Because right now it's only 50% or 60% of which usually go to vote. I think it would motivate people to participate more.

Researcher 1: Would you personally be enforced to participate more?

Subject 4: I do anyways. But yes I think it would make the process easier.

Subject 7: Probably without the proper knowledge of the technology of blockchain not everyone will be encouraged to vote. I mean someone who doesn't know how this kind of voting app works, especially the older ones, are not so encouraged.

Researcher 1: Does it apply for you as well, actually?

Subject 7: No I was trying to understand blockchain a while ago. So I was quite informed about it.

Researcher 3: But this is for blockchain specifically or online elections in general?

Subject 2: I think that this is a really good option for smaller elections like this one. For this one it is the best because we don't need a table in the main hall, signing three papers to put a small cross, in this case we only had one list, so it's more like a formality. So for this it is the best system. I don't think it can be used in larger elections like national ones. Not just because the problem of older problem. That's also true but also because I think people won't feel safe enough voting for such an important thing as national elections online.

Researcher 1: Would you personally feel safe?

Subject 2: No. Personally, in my opinion I wouldn't feel safe. I know that the system that we use now, at least in Portugal that's the one I know, is a little bit old fashioned of course. Putting the paper in a black box but I feel safe to do that. I know that will be counted four or five times from different people right on the day. Then a few days after the votes are checked again. So, I know it's old fashioned and costs a lot of money but the vote will actually be counted as it is. In the online system for small elections like here, nobody will try to hack the system. It's not worth it. But in a large election it can happen.

Subject 5: I actually share your opinion. It's simply easier to understand the old fashioned system we have right now. Mostly it can't be rigged and I understand this. But I don't understand blockchain and how it works. Of course, nobody should be able to rig it but because I don't understand it, I don't trust it.

Subject 1: I basically disagree with it. I don't have any deeper understanding of it. But someone explained me how blockchain is actually working and I think also for big votings, like for the EU where we had a traditional system, even there were problems with some votes. I think the blockchain method might be even better for elections like this. I mean I don't have data but the risk of losing votes is even less because in the EU election where they counted the votes traditionally, they also had miscounted votes.

Researcher 1: So you would be happy for the next government election in Germany for example if they come up with some online system?

Subject 1: Definitely.

Subject 6: I think it's all about transparency. I know blockchain, so there was no problem with it and I felt fine with it. I thought it was secure. But some of my friends were like "I don't know how it actually works. So how can I know it will be safe". People won't search for knowledge about it. So, I think you need to educate people.

Question 2*: Researcher 1:* So you actually helped me to make the transition to the next question. So the next thing we were interested about is, do you think that as you mentioned transparency is crucial, important or does it even affect your attitude towards online voting? Or does it have no relationship with it? Is there anything transparency can make it more likely for you to participate in online voting or make you feel secure with it?

Subject 3: I think that's pretty much the key to implement online voting in any election. That's also the only or one of the big advantages compared to traditional voting. Because there you also don't have the transparency of the people who are actually counting the votes. That might be the key to actually be able to convince people to trust it. But I also agree with other points raised where there might be hesitation for many people to use it. But it might also be the case it's getting more people to take part in elections compared to traditional voting.

Researcher 1: Any other views on this?

Subject 7: Transparency is the key requirement for voting. Not only for online voting.

Researcher 1: So that means if there would be a system which is 100% transparent, you would definitely be more likely to participate?

Everyone agreed

Subject 1: I think blockchain is ensuring transparency even more than people who are counting the votes because as a normal citizen you don't observe them and count with them and checking if they are doing the right job. But if you have blockchain technology, everyone knows how it's working and can see online everything is saved, it's even more transparent.

Researcher 1: Do you guys agree with this or do you think it's more transparent if we stick with the paper ballot system for example?

Subject 5: I think it would be more transparent if you change to blockchain. Because you guys did it that everyone can check their vote. When I put in my code, I didn't really understand what I'm seeing but if you're explaining the people what the information actually means I thought it's really cool that you were able to see your own vote. So, if everybody could do that, I think it's transparent.

Subject 4: It's just like a list of 10 million voters in a country. Then you can see anonymously this code voted for this candidate or party or for some specific cause. I think it's definitely more transparent.

Subject 3: But then it's still just something virtually that's displayed and not an actual ballot you can have in your hand. I feel like you have to get to a point where people actually trust the transparency you are promoting and that's the tough part.

Subject 7: I actually have a question. Blockchain technology is what's in between you and the candidates. So it cannot be hacked. But what about the mobile phones, for example? That's the most vulnerable point right? I mean the blockchain is trustworthy but the actual device is not that safe right?

Researcher 2: It's definitely a point of attack. The device you are actually entering the vote is the most vulnerable part of the whole system. Once it is on the blockchain and it's distributed, the security is really high. But the individual devices are definitely a point of attack.

Question 3*: Researcher 1:* So, thanks again for facilitating the transition to the next question. Talking about blockchain, the next question would deep dive into the technology. What's your opinion about blockchain in general? Some of you already mentioned you didn't understand blockchain? Do you roughly understand the idea and concept behind it or don't you have any clue? Does someone might even have advanced knowledge?

Subject 6: I would say I kind of have an advanced knowledge. I know how the network with all the nodes works. I know what happens when you just try to change information on one of them, how hashed are created and that it creates a great layer of security.

Researcher 1: What about the others?

Subject 4: More or less the same. I would say a bit less based on the programming course at University.

Subject 2: I didn't know anything about it. At the time that I was voting, I really didn't get the point of what it is and spent like 10 seconds on what it is and skipped through. It is not about my vote, just let me go. But I just realised right now, based on your explanation, what it is. Thinking about what you are saying about it right now, made me realise what blockchain actually it is.

Researcher 1: Anybody else wants to share their knowledge about blockchain?

Subject 1: The only thing that is in my mind, is that it's more secure. I think it's really difficult to hack and I rather trust a system that is really difficult to hack than a human being taking over my vote.

Researcher 1: If nobody wants to add anything to this, we would more specifically go towards our or your voting experience, respectively with our system. So probably, let's start with summarising with everything you said so far. Where you in fact confident that the system cast your vote correctly as it was supposed to be casted?

Everybody raised their hand

Subject 6: The verification at the end made me feel more confident about my vote actually being casted correctly.

Subject 1: I totally agree.

Researcher 4: Can everyone raise their hands who actually verified their vote?

6 out of 7 subjects raised their hands

Researcher 1 asked Subject 3 directly who did not raise the hand: But you were still confident that your vote was casted correctly?

Subject 3: Yes. In this election, yes.

Question 4: *Researcher 1:* Let's imagine exactly the same system for your next government election. Would you feel the same based on your experience?

Subject 5: I just thought for a student representative election it's just not that important. Nobody would have an interest except the candidates and I don't think they would actually rig the election. But for a nationwide election, I wouldn't feel so confident right now.

Researcher 1: So if I get you right, you only believed your vote was casted correctly because you thought the likelihood tries to hack the system is low?

Subject 5: Right.

Researcher 1: So, if you would participate in an election were the likelihood is higher, you would not trust the system?

Subject 5: Yes, exactly.

Subject 2: Yeah, I have the same opinion. I also thought it is completely safe and I also verified my vote. But it is just for this specific election. In a national one, I am absolutely sure I would not going to feel safe. Especially because there are more advantages in hacking the election than it has in this election. Also another problem is the thing that someone said earlier with the trust in human beings. Actually in our system right now, even if you can cheat something, you just do it in a specific polling station. And in Portugal you can vote in thousands of different paces. So even if you cheat somewhere it's just a very small percentage. With the system, it's just one system and even though it will be huge, it's one system for 10 million votes. If you can manage a way to enter this system, although it's hard, you have access not just to one thousand votes but 10 million. The damage can be in a large scale because of that.

Subject 4: One question. Do you know if a blockchain has ever been hacked?

Researcher 1: There are cases with bitcoin. Bitcoin's also work based on blockchain. There were some cases some years ago where some exchanges got hacked and attackers successfully stole bitcoins from them. In other words they hacked their accounts or wallets respectively and not the whole blockchain.

Researcher 3: The difference here is important to say. They hacked a specific account and send bitcoins from one account to another basically, not the whole blockchain. Translated to our use-case it would be one vote.

Subject 3: So they basically changed one single vote with huge effort?

Researcher 2: Translated to our case, yes.

Researcher 1: In other words you were not able to hack the whole (voting) blockchain but able to influence single blocks. In our case, there was one transaction/vote per block. Normally there are multiple transactions in one block and sometimes there were even able to change some transactions of one block. Considering the whole blockchain this is a considerably small part but still there should be mentioned.

Subject 1: Just one comment on that. Correct me if I'm wrong. If we would use the blockchain method for national elections, the more people are involved the more difficult it is to hack right?

Researcher 1: Yes. That's a principal of blockchain. The more people or nodes participate in it the higher the amount of connected devices is and the harder it is to hack the blockchain.

Subject 1: So, the more secure it would also be, no? So it would be the exact opposite of what we just said right?

Researcher 1: True, but the bitcoin blockchain was considerably large at the point where people were still able to hack specific accounts as well. Talking about having a blockchain based election on a governmental level, there is probably the need for some kind of administration or technical adjustment in order to make it secure.

Subject 7: In your system, who actually did the mining?

Researcher 2: We actually had no miners in our system. Our system was based on the blockchain logic regarding the hash system and connection between all the blocks but it was distributed. We did not have miners in between all the nodes checking each block and nodes who are checking back and worth in order to get to a consensus. There was no need for miners in our basic version. If you would go to a larger scale, like a nationwide election, there has to be a consensus protocol!

Researcher 1: We are already answering our next question. Maybe each of you could more specifically state, if you had any doubts about the system, what would have been the reasons for that? Are there any specific reasons creating doubts in the system or your doubts only connected to a use case of a much bigger scale like national wide elections?

Subject 7: Only when the scale is larger.

Question 5*: Researcher 1:* So we go on with a large, last question. Was it actually clear for you guys, at the very moment when you voted, that the whole system was based on blockchain technology including how votes were casted.

Subject 5: No, I did not know. The guys told me later.

Subject 6: From the moment on, when the hashed appeared I knew that it was Blockchain. And the experiment we conducted in class together with the professor before the election already gave me an idea.

Researcher 1: So the visualization helped you to believe that it was actually based on blockchain?

Subject 6: Yes, exactly.

Researcher 1: Did for you, Subject 5, the visualisation help to understand that it's based on blockchain?

Subject 5: No, seriously, I checked the code and I thought it would be my vote but I did not have any idea that it was actually blockchain. I did not have any background in blockchain technology.

Subject 6: Well, it's also not something happening in the front end. It's something happening in the back.

Subject 1: I only knew it because I was talking with you about it before. If we would have not talked about it I guess it would have been the same as for Subject 5. I still do not have any background.

Subject 2: I also did not know that it was actually blockchain.

Researcher 2: Did you spend time with the blockchain visualisations like scrolling through the votes or searching for your own vote? Or did you not use it at all?

Subject 6: I just looked at it and swiped right and left and that's it.

Subject 7: I checked how many votes there are.

Researcher 3: Did you guys read the information that was written on the webpages or not at all?

Subject 3: Yes, shortly. Well written!

Question 6: *Researcher 1:* Okay, so another small question since we are good in time. So before everybody seemed to agree that transparency is a very good way to enhance trust in online election systems. So making the transition, do you think the blockchain usage can actually increase this transparency. Or does it not have any impact.

Subject 2: I really think that it can help. Today, we do not have a lot of transparency. For example, in portuguese elections we have a lot of trouble with people who want to vote and live outside of Portugal. They have to go to the embassy, send a letter and it needs to include lots of bureaucratic documents like your citizenship card. So, it's a huge mess. So for example, a good way to start would be this case because people do not think that their votes are actually secure since they travel for miles between post office. So a good way to start getting more transparency would be here and then people will trust it and spread the word about it so that eventually everybody trusts it and is willing to use it.

Researcher 1: If I understood you correctly you mentioned before that you would not be confident with having the whole system based on blockchain online voting.

Subject 2: Yes, exactly because in terms of transparency the current system works quite well. As a result, a good way to start deploying it would be in cases were transparency is not as good as it should be. So people are able to notice that the system works quite well and is really transparent even knowing that the technology has limitations and failures. If we can deploy it in these cases, we could also deploy it nationwide. I think that it will be easier to convince people to trust the system if they could already see that it has proven itself to work in a smaller sample instead of just saying: "And now everything is going to be online".

Subject 3: I actually have a hard time imagining how you could prove to people that their online casted vote was actually counted correctly. You can say: "Blockchain did this and that" but people will still not believe you.

Researcher 1: Don't you think that the transparent view on every single vote like it way embedded in our system helps to prove the correctness to people?

Subject 3: You could literally put everything there. I think it helps but is not enough.

Researcher 1: So you think that the current, paper-based system in which you do not know at all what happens with your vote after you casted works better in this regard. We thought that the blockchain-based approach in which you can at least see something about your casted vote would help.

Subject 3: Absolutely. In the beginning, I thought that it has the potential to be more correct and transparent than human counting. But in traditional counting you still have different people with different political interests involved who control each other. I think it has potential to be involved in elections but I think it will be hard to convince people to trust it. Look at the digital impact in elections like the US presidential election or Brexit. That scares people.

Research 1: Any other opinions on how blockchain can influence the transparency of online voting?

Subject 7: Well, I'm thinking about older population. The difficulty is that they do not even know how to use an App. You can give them transparency but if they do not know how to use it, probably, they do not get it.

Researcher 1: What about yourself? Does the online voting with the inclusion of blockchain feel more transparent that before? Or did it not affect your perceived transparency of the system?

Subject 7: No, I mean I did not have the chance to use it a lot of times so it's hard to tell. I was trying to figure out what the answer would on a nationwide level.

Researcher 1: Any others who want to share their opinion on this topic?

Subject 5: Yes, I think that what Subject 2 said was quite interesting. You said that, when people are not in town then they also do not have the certainty that their vote is casted correctly since they have to use a more complicated process. So I think that if you want to make the transition to a blockchain-based voting system this would be a perfect way to start. Just explaining it to people so that people get more comfortable with it. Because right now when you are mailing your vote, you have no idea whether your vote was actually counted so I think this would be an interesting starting point. Also to convince people and show them the system's transparency. Not that everybody votes the same from the beginning on, but if you start with those people, I think that the small group together with the transparency of the system would help driving the acceptance of blockchain voting.

Researcher 1: Okay, let's make a quick hand vote. Who thinks that blockchain increases transparency for online voting? Two out of seven?

Subject 3: How do you define transparency in this sense?

Researcher 1: We agreed on that transparency is actually important for your trust in the voting system. So just use your own definition of transparency in this sense and answer the questions accordingly.

Researcher 2: Okay, now six out of seven.
Researcher 1: Alright, I think we came to an end. Thank you so much for your participation guys, we appreciate it a lot!