Blockchain based voting system with Ethereum Blockchain

Research Thesis

Presented in partial fulfillment of the requirements for graduation

with research distinction in Political Science in the undergraduate

colleges of The Ohio State University

by

Jinjie Chai

The Ohio State University

November 2020

Project Advisor: Professor Tomas Wood, Department of Political Science

Abstract

Internet Voting has been debated for years. Since the invention of blockchain, the feature of immutability makes the absolute security of internet voting possible. Ethereum provide a platform based on the blockchain for decentralized applications such as voting system. In this paper we will discuss about the problems of current internet voting and will proposed a voting system based on the Ethereum network.

Introduction

We have witnessed so many voting methods in our history, from holding up hands in an assembly in the ancient Greek era to paper ballots and electronic voting machines. The location of voting, however, is mostly unchanged. Most of us either vote in Polling station or use mail-in ballots. We have to register for each voting, and then we have to go to, if choose to vote in person, the designated polling station on designated vote day, to spend much more time than vote itself before voting. Without a doubt, the cost of voting is preventing people from exercising their right to vote. Chapter 1 of this thesis will focus on the history and the present of the voting method and voting system and conclude their drawbacks.

Since the invention of the internet, going to polling stations to vote seems archaic. Governments are trying to implement a voting system that does not require people to physically present at the designated voting station. Estonia was among the first countries to adopt an internet-based voting system in the Estonian parliamentary election in 2007, and today there are more than 10 countries implementing voting over the internet. While the new platform for voting evidently increases the voting turnout of those countries because of the reduced cost of votes, there are reasonable security concerns for the platform.

Firstly, the internet is vulnerable to anonymous attacks from anywhere in the world. Unlike tempering a physical voting machine in the polling system will leave some tracks, attacking the internet-based voting system will hardly leave a clue to find the attacker. Other types of interference for the internet-based voting system include spoofing and DDoS(distributed denial-of-service attack), which are defined as incoming traffic flooding to the server from different sources, making it harder for the regular visitors to enter the website. There are also viral attacks

on the computers of voters, which theoretically can act on anything on the computer, including helping to vote. Moreover, there are many potential ways to temper the server or modify the turnout, and hackers can do those without being noticed. Moreover, because the website used for voting is too large extent a centralized, tempering it would have a much larger impact than the current distributed polling station. Chapter 2 will access the current internet voting system and its potential risks to be attacked.

A blockchain is an immutable ledger maintained using consensus as a decentralized peer-to-peer network. It was originally proposed by Stuart Haber and W. Scott Stornetta in 1991 that aims to design a system where the data is timestamped to be unchanged. Later, Bayer, Haber, and Stornetta integrated Merkle trees into the system, which allows relevant timestamps to be printed in one block. It is Satoshi Nakamoto who truly realized the concept in 2008 in his famous Bitcoin Whitepaper. Bitcoin is a peer-to-peer electronic cash system, where the transaction does not go through a trusted third party. To avoid the double-spending problem, meaning you may use the same token twice without a trusted third party verifying, the bitcoin network used a hash function to encrypt every transaction with a timestamp and integrated them "into an ongoing chain of hash-based proof-of-work" (Satoshi,2018)a predetermined consensus rule for the system, forming a record cannot easily to be changed unless redoing the proof-of-work, which is extremely hard to achieve. Chapter 3 will introduce the underlying encryption techniques for blockchain and how it would be the safest under different situations.

The irreversibility of blockchain coincides with our demand for an online voting system. If voting results cannot be modified, the reliability of such a system would be the best than any other voting system we ever had in human history. Moreover, Voters with permission in this system can remain anonymous in the digital voting entirely, whereas, in traditional voting, you

will always interact with people at the polling station and may leave a record. In addition, the result is fully transparent and verifiable to the authorized people depending on the specific design of the voting system. Last but not least, the processing time and the cost for voting would be minimal compared to the huge budget the government invests in voting.

We can further improve the blockchain-based voting system by introducing smart contracts in our system. The smart contract is another important feature added on the blockchain which the term was coined by Nick Szabo in 1997. Initially used for computation purposes on the blockchain, the concept was developed by Vitalik Buterin in his blockchain-based platform Ethereum. Using the platform and its own programming language Solidity, a voting contract could be built before the vote, and authorized people could perform a vote-tally using its self-tally feature. Chapter 3 will also discuss the feasibility of an Ethereum platform voting and an example of a simple voting contract using solidity.

Blockchain-based voting, though it seems extremely safe and autonomous, will have fatal problems if not designed properly. The consensus, for example, "proof-of-work" is based on the simple majority consensus of participants. However, if a single or a group of entities controls more than 50% of the computing power, they can do double-spending——which, in our case, double voting. This is an extremely rare situation but can be addressed properly by changing consensus rules at the time of designing the system or, as a last resort, hard fork, which essentially paste the blockchain right before the unauthorized.

Similarly, smart contracts have potential problems. Not only can we write contracts on the blockchain to cast voting, but also, we could write contracts for buying votes. Unfortunately, using smart contracts, criminals can ensure the vote to be assigned their desired candidate, and

only by doing so will the criminals give the money to the voter. Unlike in traditional voting, in which those buyers can never ensure their desired voting, using smart contracts can ensure it unless the voter does not want the money. This can be prevented by encrypting the choice of vote using a method that only the administrator (in the smart contract, we can always assign an administrator) to decrypt. By doing that, those vote buyers would never know, like in traditional voting, whom they vote for. In the discussion section of chapter 3, we will discuss the potential risks of implementing a blockchain-based voting system and provide possible solutions to them are.

Chapter 1 The history and the present of Voting system

In the field of political philosophy, it is debatable whether the act of voting is worthy for voters themselves as a means to exercise democracy. The most famous theory, "paradox of voting" by Downs in 1957, states that it is surprising that every vote, even if they change the election results a little and given that it cost so much time to get to the ballot station and vote. For example, according to the United States Election Project in 2018, the total ballot in the 2016 presidential election was over 13.8 million, which means one vote only counts for less than ten million of the result. As a contrast, the time spent on voting, from a survey conducted in 2016 during the presidential election by MIT Election Lab, was on average eight minutes. It seems, according to Downs' theory, that the cost of voting cannot produce the maximum output. There are typical responses to the paradox of voting; for example, voting is merely changing the "mandate" of the candidate. However, to address the paradox fully, the only effective way is to reduce the cost of voting. If voting is merely a click on the cellphone that spends only less than a second, the paradox will be implausible. It is apparent that an electronic(internet) voting system can reduce the cost of voting substantially; thus, it is imperative to adopt it to solve the paradox of voting.

Policymakers are aware that improving vote efficiency is crucial for motivating voters. Conventional electronic voting, which only involves electronic machines either in the stage of voting or vote-tally phrase in the poll station, is dated to 1889 when the lever machines were

used in an election by Jacob Myers in Lockport, New York (Arnold,1999). According to Anandaraj and Sakthivel (2015), The voters will enter the machine and pull the lever, and will be locked in the machine to cast a vote. A selection is made, the lever will be pulled up, which will increase the appropriate counters for candidates. Such a machine was predominant by 1930 in almost every large city in the United States (Lelia,2003). The drawbacks of the lever machine applied in voting are obvious: It has a more complex voting procedure, from the opinion of Anandaraj and Sakthivel. However, it also reduces the overall time for the entire voting procedure, including the voting-tally phrase. Because the lever machine is a large machine, Anandaraj and Sakthivel also suggest that it is expensive to test and maintain.

There is another widely adopted electronic voting system called the punched card and is still used in the present day. Voters punched holes opposite their candidate in their card, which is provided by the ballot station. It evolved to be the automatic machine by IBM in Mid-1960, and the updated one is still used in 2 counties in Idaho in the 2014 General Election (VerifiedVoting,2019). It has several advantages over the lever machine, including less maintenance, is required, and easy to store. (Selker,2004)

It is worth pointing out that those voting machines or mechanisms are reducing the overall voting time, including vote and vote-tally phrase, by focusing on reducing vote-tally phrase. They virtually increase the cost of voting for voters themselves. As a result, we can expect that those two kinds of voting machines cannot motivate people by simply reducing the time for the voter-tally stage.

It is the computers applied in voting that reduce the time of voters. Direct-recording Electronic (DRE)voting system is still used in every election in most of the states. Most of DRE system

used in the United States is accompanied by a Voter-Verified Paper Audit Trail (VVPAT) which allows voters to "verify that the choices indicated on the paper record correspond to the choices that the voter has made in casting the ballot"(National Academy of Sciences, 2005). Voters can see a ballot display on the monitor of the machine and select whomever candidate they want to elect. The drawback of a machine without VVPAT is that it is not auditable, and its built-in code may have potential bugs that lead to malfunctioning. For example, in October 2019, During Governor Election in Mississippi, the voter Ethan Peterson was trying to vote for Bill Waller Jerome as the next Governor of Mississippi, but the DRE voting machine in Lafayette County repeatedly selected Tate Reeves instead (Newsy,2019). Moreover, the DRE is vulnerable to be hacked. Researchers from Argonne National Laboratory in Illinois Claim that it only costs $26 to hack an ordinary voting machine that is widely used in the U.S.Meanwhile, A DRE with an audit trail seems to cost more than the traditional paper ballot because it involves an audit procedure.

The voting methods and machines mentioned above do not satisfy either of minimizing the cost of time for voters or the cost of vote-tally phrase. The lever machine has a complicated voting procedure and costs much to maintain. As for punched cards, it increases the overall vote time for voters. Moreover, DRE seems convenient, but it may be hacked or cause the error as we see many examples in reality. A DRE with an audit trail may be secure, but again, it costs much more in the audit procedure than that of a traditional paper ballot.

So, is there a voting system that substantially reduces the cost of voting, meanwhile, increases the efficiency of the voting-tally procedure, as well as committing to the sincere choice of those votes? Some might say a sophisticated internet voting system would save us.

Chapter 2 Evaluation of current Internet-based voting system

It is imaginable that once an Internet-based voting system is implemented, the voter turnout would skyrocket, for it does not require voters to stop by a polling station to exercise their power. However, political scientists and computer scientists will not give up the security of voting results in exchange for the convenience of voters to favor an insecure internet voting system. There are reasons why policymakers are conservative in implementing such a voting system.

Among those, one of the intuitions is that the whole voting process is invisible to most people. Firstly, it is invisible because it is hard for the public to understand the techniques behind it. While conventional voting systems at present also depend on computers by converting the decisions on the candidate to the databases of computers, the decision of voters using an application will be directly entered into the voting database. Besides, the internet voting system will also include more codes from different election stages. The process of how those data are recorded and manipulated into the database is intricate for the public and is less comprehensible compared to the way we record the data in conventional voting. To establish the trust of constituents, organizers want to ensure the voter can witness their vote. In other words, voters are always concerned that their vote "counts." In a conventional voting system, for example, the DRE with an audit trail voting system, which is implemented in the majority states of the U.S nowadays, Organizers are addressing this concern by providing a print-out version of the choice of voters before they are casting a vote. There is no internet voting system, however, which provides such records to the voter while they are casting their vote online.

Another issue concerned is about the voting environment. In conventional voting, staff members are monitoring when the election is ongoing. Any attempt to tamper with the voting device will be detected, and alternative solutions will be implemented. However, the voting environments when implementing internet voting are complicated and might be beyond the control of the organizer. Specific to the internet voting system, the environment can be referred to as two perspectives: physical voting environment and device voting environment. For a physical voting environment, it cannot be assured that the vote is out of the will, if not witnessed by the organizer, like in the polling station. Voters may be under the influence of alcohol or coerced by someone to make an involuntary decision. Organizers cannot ensure the safety of the voting environment. Moreover, it seems that organizers cannot control the device environment of the voters, either. Devices, such as desktop computers or smartphones, may malfunction while voting or being hacked by a virus that can control the voting. The virus could potentially hack into the computer of voters and make choices or changes against the will of the owners. All in all, those who favor conventional voting do not want a system with many potential risks and situations that organizers cannot control.

There is another interesting consequence of lacking control of the voting environment. Selling votes and verification of selling votes would become efficient in the internet voting system. Although it is a common problem in all voting systems because the voting process in conventional voting is under the surveillance of the organizer, it is hard to verify a vote-selling. While in the internet voting system, one could provide their username and password to the buyer under some internet voting system that does not require face recognition. Another way that vote sellers can prove their choice is to record the entire voting process and provide it to the buyer. It

seems that the internet voting system is ideal for vote buying/selling, as well as for vote swapping.

From the perspective of the internet voting system itself, we cannot see, those opponents argue, whether the internet-based voting is secure, even if the makers claim it is invulnerable. The most severe attack would come from the insider, who can access critical databases for an election. Insiders can easily modify the result by changing the data in the database, which would be undetectable if done by a skilled hacker. Furthermore, even if it is free from data modification, it can suffer from other kinds of service disruptions. For example, a denial of service attack (DDoS attack) is a low-cost method that can prevent legitimate voters from casting a vote on the website.

Other claims from opponents include that we cannot even detect whether the data in the system is modified or not since there are no robust verification mechanisms behind the internet voting system. While the malfunction of voting machines could be detected and the machine could be stopped to use for maintenance during the election, it is crucial for the internet voting system to run during the election. That means the server, database, internet, and other components of the internet voting system Should be in good standing in the entire voting process. Unlike voting machines distributed in various polling stations, It seems that the internet voting system will only be functioning as a whole.

It seems that while we reduced the amount of time wasted going to the polling station, we are risking ourselves into several potential problems in the internet-based voting system. Not only organizers cannot control both the physical and computer environment of the voters, but also the voting system itself is vulnerable to be hacked or modified, both from insider and outsider,

which the latter can be anyone or any organization in the world. It is afraid that the server will be like any other server in the world, malfunctioned in the critical moment. It seems that part of the potential problems can be solved by introducing a new concept into the internet voting system, called Blockchain.

Chapter 3 Introduction of a possible blockchain voting system based on Ethereum

As introduced earlier, blockchain is, by its name, a series of growing blocks chained together. In a typical blockchain, every block contains the hash function that is dependent on the previous block (except the first block), a timestamp, and transaction data. It requires consensus in the network to change any of the data, which is nearly impossible. As Rifa and Budi point out in their paper Blockchain-Based E-Voting Recording System Design, "The block is related because from the previous hash used in the next block making process, the attempt to change the information will be more difficult as it has to change the next blocks"(2017). The blockchain-based voting system can appear to be as simple as a normal online voting platform to the voter, however, implemented blockchain technology in the back end. A voting system has many components, including voter registration, election form configuration; in this paper, we will only discuss the design of the vote phrase and tally phrase. Implementing the blockchain concept in the voting system seems promising; however, we must design the safest voting system that is immune to any chance of changing any voting data.

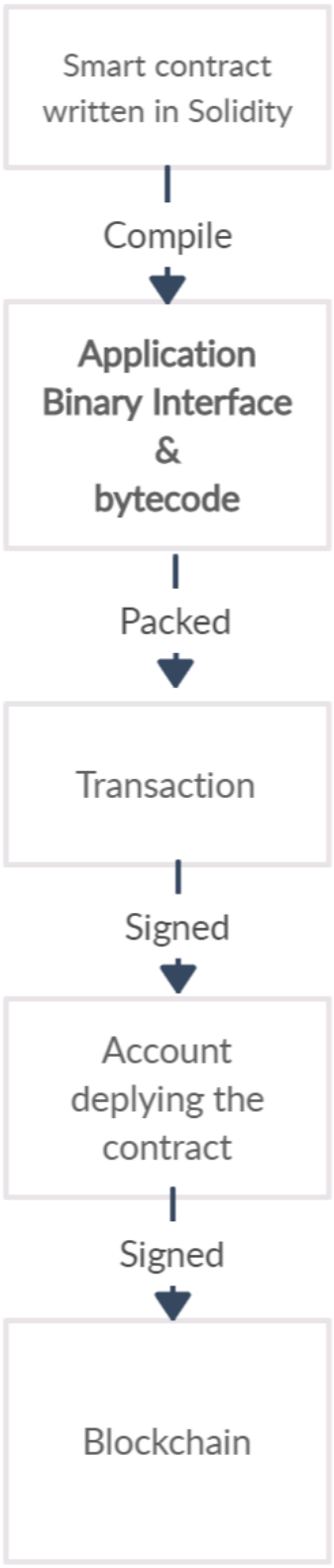
There are many variants of blockchain techniques and concepts that we could incorporate into the voting system. It is also possible to build an independent platform for a voting system, although the cost of it would be higher than utilizing an existing blockchain-based platform. In this paper, we will implement an existing blockchain platform as the level of 87 security would be as same as the platform that we built from scratch. While Bitcoin is undoubtedly dominant in the area of cryptocurrency, it is not fit for other applications to run on the bitcoin ledger.

Here we want to introduce Ethereum as a backend in the voting system. As the figure shows(figure 1), the blockchain-based voting system could appear as the same as the current internet voting website showing for voters but implement, rather than traditional database, Ethereum based blockchain platform.

Ethereum was founded by Vitalik Buterin in 2013 and was described by the founder as a "Next-Generation Smart Contract and Decentralized Application Platform."(Vitalik,2013) In other words, Its aim includes providing a protocol for building decentralized applications(DApps). There are three types of applications that are suitable to run on the Ethereum platform largely because of the advantage of smart contracts that are embodied. The first kind is financial derivatives like futures and options, which can be automatically transferred or executed. The second kind of Dapps that can run on the Ethereum platform is semi-financial, where the money is involved, but there are other non-monetary situations in the application. Our design of the voting system is attributed to the third kind, which does not involve money but only a series of events.

The smart contract is the most prominent feature on Ethereum. It is written in the Solidity language that was introduced by Vitalik with a combination of C++ and javascript. The smart contract is provided in the Ethereum network that enables it to execute without a traditional server but runs through Ethereum virtual machine. Like the process of Java Code, a smart contract written in Solidity language will run through an Etherrum virtual machine and be translated to Application binary interface (ABI) and Smart Contract Bytecode. The former is used to interact with solidity and bytecode, and the bytecode is packed with other parameters into a transaction. The transaction will be signed and be put on an Ethereum block once deployed.

Below is the flowchart of how smart contract deployed on the Ethereum blockchain.



We want to discuss how and at what stage that smart contract could play a role in a voting system. We will take the US presidential general election in this paper as a typical example of a voting system. Although under the US constitution, presidential election voting is organized at the state level. It is up to each state to decide whether to implement Ethereum at all or use the platform partially in some stages of the voting process. We will design for each stage of the voting process independently and have an interface between them so they can access the database from each other(some may be unidirectional).

Design principle:

Eligibility of the voter and the vote: only registered voters are eligible to cast a vote in a specific session of the election. When performing voting, only registered voters with additional verification right before the voting can cast a vote. Every vote is counted. There will be no invalid vote of any kind if a vote is tallied and cast by a registered and verified voter.

No multiple voting is allowed: It seems to be an issue for online voting that some multiple voting from one voter is inevitable; in Blockchain-based voting system, especially the one that implemented Ethereum as the platform, it is easily prevented: Once an identified voter(with unique ID) cast vote, the status of the voter will change to "voted"(or other forms of "voted"), which under this status the voter cannot cast another vote, but can only verify the vote cast.

The integrity of the vote: No one can modify the result of any vote.

Source code must be published: Source code of the entire voting system should be reviewed before implemented.

Privacy of voters: Although the voting system source code is public, all data involving voters and votes must be stored in a database that is not public.

Proposed Voting schemes:

First stage: voter registration. Before the general presidential election, all eligible voters need to register to get the ballot. Up to now, online voter registration is enabled in more than 40 states in the U.S. Having the existing database of resident transfer to the Ethereum platform seems reasonable and convenient for the election officials. Another way is to have an interface connected with the voting smart contract to determine the eligibility of the voter. Either way will enable the database free from unauthorized modification. Moreover, biometric information such as photos is needed for voter verification before casting a vote.

Second stage: voter verification. Voters can either go online or use mobile applications to cast a vote. Before casting a vote, facial recognition may be used to verify the identity of the voter. Other verification could also be used if they can verify the unique identity of the voter.

Third stage: vote stage: verified voter(encrypted with ring signature*, which keeps the voter anonymous when voting, also allows observers to tally the vote without knowing any identity of voters) cast a vote from a list of candidates once.

* invented by Ron Rivest, Adi Shamir, and Yael Tauman, and introduced at ASIACRYPT in 2001, a Ring signature is a type of asymmetric cryptography that keeps voters anonymous when observers tally the vote.

Fourth stage: Vote validation: check again for voter verification and mark the status of voter change to “voted”.

Fifth stage: Vote tally and count: the vote is counted to the database. Observers other than administrator tally the vote.

Voting system components:

Corresponding to different voting stages, there are essential components for the designed voting system. For the user interface, web and mobile applications are needed for the voter to register and vote. They can be either integrated into one website or application or using several depending on the law of each state. For the backend, a database server and smart contract should be implemented.

Implementation of smart contract and discussion

Here we will only the core component of the voting system for the smart contract portion, and we will discuss its performance and cost.

Implementation of smart contract and discussion

Here we will only the core component of the voting system for the smart contract portion, and we will discuss its performance and cost.

Roles and rights

Although our application(or smart contract) is a decentralized one, we still need an administrator(in Ethereum platform called “the owner of the contracts”) who cannot manipulate any ongoing election, but can initiate one and set the condition for the end of the election. More importantly, this administrator can determine who is eligible to vote before the set event is started.(Right hand side is the pseudocode for the features that administrator have)

```
Struct administrator {
Address ID
Function
initiateNewElection(Uint
Startdate,Uint endDATE,
Address administratorID,
List Address Candidate
ID)
Function
RegsiterVoter(Address
ID)
}
```

Another role is voter, which has a state of “isVoted” and “isVerified”. Voters will be added to the database and will be assigned a unique address. Each election administrator will assign a unique address every time for a registered voter. Before every voting, the voter needs to be verified by biometric information in order to get the status of “isVerified” changed. Only a verified and voted vote will be valid. (Right hand side is the pseudocode for the features that voters have)

```
Struct Voter {
Bool isVerified;
Bool isVoted;
Address ID;
Function Vote(Address
VoterAddressID,
Address CandidateID);
}
```

```
Function Vote(Address
VoterAddressID, Address
CandidateID)
If (Voter.isVerified
&& !Voter.isVoted &&
CandidateID&&
now >=Startdate &&now
<=endDate)
{ Candidate.voteCount++;
 Voter.isVoted = true;
```

For voters to vote, they must be verified, and the time of voting is later than the set start date and before the end date. Then they will be marked “is voted” and their choice of candidate will have one more vote on their voteCount Variable. (Right hand side is the pseudocode for the vote function)

Within the function of initiateNewElection, there is a list of candidateIDs, which contains vote count and a Boolean status of winning the election (either true or false). The winning condition is when the end date passes, the most voted candidate will be labeled by the Boolean variable “win” true, thus winning the election.(Right hand side is the pseudocode for the features of candidates and the winning condition)

```
Struct Candidate{
Address ID;
Int voteCount = 0;
Bool Win = false;
}
Function Win(List Address
VoterAddressID)
if(now>endDate)
{
max(Candidate.VoteCount).C
andidateID.win = true;
}
```

Discussion

We could see based on the Ethereum platform, our coding language solidity of smart contract is like JavaScript, with addressID feature. That is because the Ethereum structure has already done the immutability and the platform is favored by many developers. Notably, every transaction needs the miner in the network to confirm, and often multiple times. In our case, every transaction, and every recording, including register people eligible for vote, needs to be confirmed and time stamped by the miner in the network. It cost “gas” to confirm every transaction in the Ethereum network to keep the platform running. Gas is the unit of measure for the amount of work that is accomplished for an operation and the gas price is measured in terms of ether in Ethereum network (Buterin et al., 2013). A million of additions or subtraction, according to Buterin, cost three million gases (about 5 dollars for the current Ethereum cryptocurrency price). But if we want to store the data as large as the registered voter for the U.S.

presidential election, it could cost millions of dollars. But it is still substantially less than the election that we held today, which cost billions of dollars.

Further Improvement for the core component

First, those chunks are pseudocode, which is not an actual application of a voting system. If we make an actual application, we could find out the performance and the actual cost of a simulated election. Secondly, the model we proposed should add ring signatures to protect the voter privacy when voting, and that can be discussed in other scholar's models.

Potential challenges to the Ethereum platform

As we determine to design a voting system based on the Ethereum network, we trust that the Ethereum network, under any circumstance, will maintain its immutability. Some situations may be theoretically possible; however, they are prevented in the real world.

51% and 67% attack

Under the consensus of proof of work, if a group of miners in the network controls more than 50% of the mining computing power. They could determine to either halt any transaction they wanted or do the transaction twice. In our voting system case, they could either halt any voting activities, or they can also vote twice. To prevent such issues, Ethereum changed their consensus to proof of stake in 2020. It will punish the actor with fraudulent transactions such as confiscating all the stake of the actor.

Quantum computer

Quantum computers are developing, and it has tremendous power over the traditional computer in some perspective. Some may say that once quantum computers emerged in the blockchain network, it may become a threat to the applications and transactions that run on the blockchain. However, unlike proof of work, where the computing power is the only factor that miner can initiate a 51% attack, proof of stake does not have such problem. Other than that, the advantages of quantum computer only limits to certain tasks like integer factorization and discrete logarithm problem, which does not relate to the computing power defined by either Bitcoin or Ethereum network. So, quantum computers would not pose a threat to the future of the Ethereum network.

Reference

Anandaraj & Sakthivel. (2015). Secured Electronic Voting Machine Using Biometric.

Arnold,Ed.(1999). History of voting system in California.

Buterin, V. et al. (2013). Ethereum white paper

Downs, A. (1957). An Economic Theory of Democracy, Harper and Row, N.Y., 1957.

Jane Susskind. (2017). Decrypting Democracy: Incentivizing Blockchain Voting Technology for an Improved Election System, 54 San Diego L. Rev. 785

Lelia Barlow (2003). An introduction to Electronic Voting.

National Academy of Sciences (NAS),2005. tp://www.ncsl.org/research/elections-and-campaigns/voting-equipment.aspx

R. Hanifatunnisa & B. Rahardjo.(2017). "Blockchain based e-voting recording system design," 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), Lombok, 2017, pp. 1-6, doi: 10.1109/TSSA.2017.8272896

Rivest, R., Shamir, A., and Tauman, Y. (2001). How to leak a secret. Advances in CryptologyASIACRYPT 2001, 552–565.

United States Election project (2016). 2016 November General Election Turnout Rates. From http://www.electproject.org/2016g

Valimised(2019). Voter turnout in Estonia. From https://rk2019.valimised.ee/en/voting-result/voting-result-main.html

Verified Voting. (2019) Video Shows Voting Machine Malfunctioning in Mississippi. From https://www.newsy.com/stories/video-shows-mississippi-voting-machine-malfunctioning/

Newsy