## Introduction

Petition systems have always been a means of conveying public opinion to those in power. In the twenty-first century, petitions are one of the most regular forms of political participation[1], with the development of the Internet, e-petitions are becoming more and more popular. The most popular e-petition system is the UK parliament upgrade e-petitions systems in 2015, it received over 30,000 e-petitions, and also 14 million people signing at least one petition[2], becoming the highest usage parliamentary e-petitions system in the worldwide. At the same time, there are many petition sites to help people start and run non-political petitions. The e-petition system is expected to solve some of problems with paper-base petition system.

First, the paper petition ballots are counted by Counting Agent, which has possible to change the number of votes accidentally or intentionally. Second, since the counting process and result are managed and stored centrally, the public is hard to verify the correctness of the paper petition result. The petition result would be incorrect due to the paper petitions have possible to get lost in the mail by accident. Compared to the traditional petition system, the important point is the process and result of E-petition are open, transparent. Since 2015, UK government builds a website for each petition, which people can check the list of actions and result, and the final solution that supplied by government \cite{ref20}. This method has some effective, but the imperfection is people cannot verify the sign and the result, they may speculate about the process and result. Meanwhile, the number of signs have the possible to modification because there is no measure to protect the data unchangeable.

Base on above problems, it is expected to use blockchain to build the model. Blockchain technology achieves decentralization through the participation of members of a distributed network. There is no single point of failure, no single user and group can have control, and the data entered on Decentralized Blockchains is irreversible, which means anyone can participate and validate the data. Petitioners and people who pay attention this petition can check the process and result at anytime, and jointly supervise this petition’s fairness and justice.

Since 2015, UK government strengthen the accessible, linkage\cite{ref20}. People do not have to sign up and be audited, they just need to write a description in 380 words to submit their petition. This approach increases the enthusiasm of submitting the petition, but many of petition descriptions are unclear and one-sided. The main problem of this method is it cannot guarantee each petitioner just sign one time. Australia government tries to solve this problem, the e-petition system in Australia uses statistics on addresses, IP addresses, or email addresses \cite{ref14}. Some important petitions from government need to use personal ID to verify personal information, and petitioner cannot sign their petition anonymous. This privacy information is used multiple layers of encryption to protect as usual. The cost of this approach is proportional to the number of petitioners, and the system is prone to failure if the number of petitioners is large. At the same time, people worry that their information will be leaked if database is attacked. Also, some people would not like to sign the petition when not anonymously. To solve the problem as above, there are petitioning systems that combine blockchain and JavaScript\cite{ref15}. This approach can make sure the process and result of the petition is open and verifiable, but it cannot guarantee the fairness of the petition because JavaScript only limit one device, one sign. It cannot limit petitioner sign again on other devices. However, it is still not solved how to protect people’s information. Therefore, the anonymity mechanism needs to be improved.

The stronger anonymity is the most necessary part of the E-petition system. The basic property of E-petition system is protecting petitioner’s security information, which can prevent them from being illegally obtained and used for improper conduct, such as phone and Internet fraud and harassment. At the same time, petitioner do not have to worry about others knowing they have signed. Many of petitioner do not want other people know their personal position and point of view \cite{ref21}.Two functions above are the core of the anonymity, and their protection would encourage people participate in voting actively. To ignore duplicate signature and keeping petitioner anonymity, one-time key signature in blockchain is expected to use, which can limit one people can just sign one time but keep signer remain anonymous.

Higher anonymous means higher attack risk, petitioners and managers always worry about the data and personal information being hacked \cite{ref21}. This concern is also One of the things that keeps people from petition.

This problem will be expected to use the property of traceable to solve. Traceable is an important function that protect the fairness of the petition. Attackers take advantage of possible system vulnerabilities to break some rules, such as malicious ticket brushing, deleting others' signatures. Tracking system will trace attacker and the invalid signatures, then recover the signature and ban the attacker.

An additional function that e-petition system can be set is classification. Traditional paper petition hard to statistic the signatures of different groups. Each group of petitioners have the different perception of the issue, beliefs, values, signing practices, and live under material conditions, among others \cite{ref20}, which make the different result of the signature. If the outcome of the petition is studied in isolation, the will of the minority group regarding the petition and its appeal will not be paid attention to. The result will be one-sided and ineffective. Recent year, many voting systems add the statistic system to look at how each group voted. E-petition system also need to add this function.

The multi-attribute can let people who pay attention this petition notices the classification of the petitioner and ratio of the petitioner groups, such as the classification of the petitioner can be the workers and student, and the ratio can be 40% and 60%. At the same time, multi-attribute can be come true “one person, more vote” in some special petition activities, such as board of director can have two tickets per person in one petition.

However, the petition system is still as plenty of critics because public’s expectations are high, and little has been achieved. Public still cannot check the result on time and verify if the result is fair. In addition, the personal information is not sufficiently protected, Petitioners are concerned that their information will be leaked on the Internet and cause unnecessary trouble. In addition, paper-base petition would have a hard time to division and statistic the petitioners, and it is difficult to arrange different group casting different number of voting. Hence, using Blockchain and Attribute-Base Signature (ABS) to build a petition system are considered. Blockchain technology achieves decentralization through the participation of members of a distributed network. There is no single point of failure, no single user and group can have control, and the data entered on Decentralized Blockchains is irreversible, which means anyone can participate and validate the data. These features of Blockchain promise that the process and result of petition are fair and transparent. In an attribute-based signature (ABS), users sign messages with any predicate of their own attributes issued from an attribute authority, which means a signature is a claim regarding the attributes that signer owning, it does not show the identity of signer.[3] The basic ABS just consider the single attribute authority, but El Kaafarani et al.[4] and Okamoto et al.[5] provide a scheme that can avoid central authority and involve multiple attribute authorities, which means different signer would satisfy different policy, and sign different messages. At the same time, Direct Anonymous Attestation (DAA) [6,7] adds a new feature called the *user-controlled linkability* (UCL). This solution avoids having a designated tracing authority but also add accountability to attribute-based signatures. In addition, it allows signers link some of their signatures with the same verifier directly and keep anonymity.[8]

Contribution

Consequently, in this paper, we aim to improve the fairness of Blockchain-based and attribute base signature e-petition systems. The contributions of this paper are listed as follows.

1) We formalize the system model of e-petition systems based on Blockchain and attribute base signature.

2) We propose a concrete construction e-petition system based on blockchain and attribute base signature. It proves that it satisfies fairness, multiple attributes, keeps identity privacy, and maximal ballot secrecy. Specifically, in our construction, we modify the blockchain-based voting system scheme in [9] and the ABS in [8] to establish the basic e-petition system and add statistical steps to complete the self-tallying part in the e-petition system.

Related Work

Most of today's e-petition systems are used by government and school departments to collect people's wishes. Some petition systems\cite{ref14} use statistics on addresses, IP addresses, or email addresses. Some important petitions from government need to use personal ID to verify personal information, and petitioner cannot sign their petition anonymous. This privacy information is used multiple layers of encryption to protect as usual. The cost of this approach is proportional to the number of petitioners, and the system is prone to failure if the number of petitioners is large. At the same time, people worry that their information will be leaked if database is attacked. Also, some people would not like to sign the petition when not anonymously.

To solve the problem as above, there are petitioning systems that combine blockchain and JavaScript\cite{ref15}. This approach can make sure the process and result of the petition is open and verifiable, but it cannot guarantee the fairness of the petition because JavaScript only limit one device, one sign. It cannot limit petitioner sign again on other devices. In addition, it is still not solved how to protect people’s information.

3. syntax

There are 3 main participants: initiator, petitioner, and e-petition system manager. Initiator can built a petition topic and publish it, also initiator can edit the requirement of the petition, such as the maximum sign number, the classification of attributes and the tickets number that each petitioner own. As mentioned before, petitioner who have different attributes will sign the different messages, representing different voting numbers. The responsibility of the e-petition system manger is maintain the system work normally, and verify the attack that system mentioned.

$\bullet\ \textbf{Setup}$ ($ 1^{\lambda} $): This step is executed to set up the whole system. It will set up a public parameters pp when input a unary string, which $ \lambda $ is the security parameter.

$\cdot$ Account Establishment: This protocol is executed to establish the user’s account. Initiator and petitioner will have the different account. Initiator needs to establish a new petitioner account if he also hopes to sign this petition. Initiator account can edit the requirement of the petition, but it cannot edit the information after starting the petitions. Petitioner account will need to input there basic information to verify their identity, and it will ask petitioners to choose the attributes they own, which can classify their attribute group. Different attributes would have different ticket number.

After establishing the account, users will get a privacy account and are eligible for signing in the next step.

$\bullet\ \textbf{Start a petition}$: After Initiator set up the information of the petition, he can start this petition and published it. People who want to join this petition will use the privacy account to check the petition.

$\bullet\ \textbf{Sign}$ : This step is executed to produce a signature if the user’s attributes satisfy the predicate. Users can use corresponding secret keys to generate a signature on the petition. Petitioner will get the reminder that their sign cannot be change and delete after they confirm the signature. Each petitioner only can sign one time, the account key pair will be invalid after the signature become effective.

$\bullet\ \textbf{Verify, Tally}$ : This step is monitored by e-petition system manager. Take the signature on the petition and verify the signature. The attribute authorities’ verification keys manage attributes that are involved in predicate. It will return 1 if the signature is valid. Then the tally system will statistic valid signature, and different attribute authority will have different count number. After the petition number is equal to the required number, it will show the percentage of each petition received and output the petition Result.

$\bullet\ \textbf{Trace}$ : This step is prevent some attacker break the process and result of the petition. The system will backtrack the block and signature and recover the corresponding commitment. In addition, the attacker account would be banned.

3.1 security notions

\subparagraph{Anonymity.}

This require that the signature secret the user’s identity and the attributes, which means no one other than the petitioner can access the voter's personal information. Petitioners can verify other people’s signature under the condition of anonymity.

\subparagraph{Unforgeability.}

Users cannot refer to signature policies that their attribute set is not satisfied to output signatures on messages, even if they collect attributes together. This policy guaranteed clustering resistance.

\subparagraph{Traceability.}

Users will be traced if they attacked the database or violate the petition policy. Their information will be published, and accounts will be banned.

\subparagraph{verifiability.}

* Each petitioner can verify whether their signatures are counted in the final result, and they can verify the validity of other people's signatures. In addition, public can verify the correctness of the process and result.

Block model.

Bilinear Group. A bilinear group is a tuple P =(), where G1, G2, and Gt are groups of a prime order p and G, and G generate G1 and G2. [8] We would like use Type-3 in [9] to build our bilinear map G1 x G2 -> Gt, which G1 =/= G2, G1 and G2 do not have computable isomorphisms.

Digital Signature. We would like to use Digital Signature (DS) scheme which called one-time signature. It is correct and unforgeability, which means the adversary can just sign one-times only if it generates a new public/secret key pair. We will use a different type of full Boneh-Boyen signature scheme according to [8], namely, BB+ scheme. The schemes are described as follows,

KeyGen(P): Choose x, y <- Zp, set (X,Y) = (g2, g2), which (X,Y) is the verification key and (x,y) is the secret key.

BB.Sign(sk,m): Take the signature sigma = g(1/x+ry+m) on massage m (-Zp. In sigma, r<-Zp and x+ry+m =/= 0. In addition, the signature sigma = (g1.h1z) (1/x+ry+m) in BB+.

Verify: In BB+ scheme, if e(sigma, X.Yr.g2m) = e(g1.h1z.g2) output 1, otherwise 0.

Non-interactive Zero Knowledge Proofs. In this system, each proof needs its own new public reference string. Common reference strings are usually not random strings. According to [8], a Non- interactive Zero-Knowledge Proof system is a tuple of algorithms for relation R. R is an NP relation on pairs (x,y) with a language LR=(). The NIZK system is composed by (Setup, Prove, Verify, Extract, SimSetup, SimProve). NIZK is required Completeness, soundness and zero-knowledge. Completeness required that the honest verifier will be convinced of this fact by the honest verifier if the statement is true. Soundness required that only those who can prove that they know the intended secret will get the information. Zero-knowledge required that no witness information is shown.

Construction of e-petition system

In this section, the construction of e-petition system is described.

In Setup algorithm, the common reference crs is generated for NIZK system. Then a pseudo-key pair (pkpsdo, skprdo) is generated for Digital Signature scheme D2. At the same time, a public parameter pp = (vkpsdo, crs, A, H), where H is the collision-resistant hash function. In account establish algorithm, a public/private key pair(pkaid, skaid) is generated for Digital Signature Scheme D1 after a new attribute authority is created. If the user id need to generate a signing key that the attribute is a, the managing attribute authority

the managing attribute authority need to sign id, a and one-way function on user’s private key skid together. This signature is the private key for user’s attribute. Then the user will this signature to sign the message that the attributes satisfied. The signature will generate a NIZK proof that the modified predicate Omaga’ will still has proper user’s attribute be satisfied.

According to the [6], the languages for the NIZK proofs are defined as follows.

*L* : { (public values pv)*,*(verify v) : Ri(pv*,*v)}

We compute the language below,

……

In [9], it describes a span program, and we use monotone span program in this paper. It is defined as follows,

##### We define a monotone Boolean function omaga : {0,1}n -> {0,1}, and a matrix in a field F has the size l X w. Then a **labelling function make a transition from l to n.**

If every (x1,…,xn) \in {0,1}n, M is a monotone span program for omaga over F, which means,-------- v is the secret vector in it.

Base on the definition of the span program, the satisfiability of omaga’ can be proved. User need to prove the property of the v \in Zp omaga’ with vm=[]. The zero element in vm is the attribute that user does not need, and user need to prove the property of the attribute and pseudo-attribute if the element is non-zero.

In Tally algorithm, CAAi need to count different times base on the petition rule. If Verify (omaga, {vkAAi}i, omaga, p) = 1, then CAAi will be counted until Sum(CAAi) get the maximum number of petitions MP. Then, the algorithm will calculate the ratio of CAAi to the MP, and output the result.

Related work

e-voting system [1]

# Bibliography

|  |  |
| --- | --- |
| [1] | A. goverment, "ELECTRONIC PETITIONING TO THE HOUSE OF REPRESENTATIVES Chapter 4 (page 41-50)," Australia, 2009. |

In Setup algorithm, the common reference crs is generated for NIZK system. Then a pseudo-key pair (pkpsdo, skprdo) is generated for Digital Signature scheme D2. At the same time, a public parameter pp = (vkpsdo, crs, A, H), where H is the collision-resistant hash function. In account establish algorithm, a public/private key pair(pkaid, skaid) is generated for Digital Signature Scheme D1 after a new attribute authority is created. If the user id needs to generate a signing key that the attribute is a, the managing attribute authority need to sign id, a and one-way function on user’s private key skid together. This signature is