A Blockchain-based E-petition system

Xiangman Li

August 2021

1 Introduction

Petition systems have always been a means of conveying public opinion to those in power. In the 21th century, petitions are one of the most common forms of political activity [1]. With the development of the Internet, e-petitions are becoming more and more popular. The most popular e-petition system was the UK parliament's upgrade e-petitions systems in 2015. 14 million people signing at least one petition, and over 30,000 e-petitions are received [2], becoming the highest usage parliamentary e-petitions system 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 the paper-based petition system. First, the Counting Agent counted the paper petition ballots, which has possible to change the number of votes accidentally or intentionally. Second, since the counting process and results are managed and stored centrally, it the public is hard to verify the correctness of the paper petition result. At the same time, the result would be incorrect due to the paper petitions could get lost in the mail by accident.

However, the petition system still has plenty of critics because the public's expectations are high, and little has been achieved. The public still cannot check the result on time and verify if the result is fair. In addition, personal information is not sufficiently protected, and petitioners are concerned that their information will be leaked on the Internet and cause unnecessary trouble. In addition, the paper-based petition would have a hard time dividing and statistic the petitioners, and it is challenging to arrange different groups casting different numbers of voting. Hence, using Blockchain and Attribute-Base Signature (ABS) to build a petition system is considered.Blockchain is decentralized through the participation of members.No single point of failure. No single user and group can have control, and the data entered on Decentralized Blockchains are irreversible, which means anyone can participate and validate the data. These features of Blockchain promise that the process and result of the petition are fair and transparent. In an attribute-based signature (ABS), users sign messages with using their attributes from an attribute authority, which means a signature is a claim regarding the attributes that signer owns; it does not show the signer's identity.[3] The primary ABS considers 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 signers would satisfy the different policies and sign different messages. This solution avoids having a designated tracing authority but also adds accountability to attribute-based signatures. In addition, it allows signers to link some of their signatures with the same verifier directly and keep anonymity.[6]

Contribution. Consequently, in this report, our target is improving a blockchain-based and attribute base signature e-petition systems. The contributions are listed as follows.

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

2)A construction of e-petition system based on blockchain and attribute base signature is described. It proves that it satisfies fairness, multiple attributes, keeps identity privacy,and unforgeability. In addition, we modify the blockchain-based voting system scheme in [7] and the ABS in [6] to establish the basic e-petition system and add statistical steps to complete the self-tallying part in the e-petition system.

2 Related Work

2.1 E-voting system

E-voting system is similar to the e-petition system, which they have the similar voting process. Voting systems have been a hot topic, and there are many blockchain-based voting systems out there. Most blockchain voting systems tend to use cryptocurrencies to vote on candidates, such as Bitcoin[9][10], and Privacy-enhancing altcoins[11] are traditional cryptocurrency-based voting systems. There are also voting systems built using Ethereum and smart contracts[12]. The Zerocoin voting system[11] helps voters maintain their privacy better. At the same time, the decentralized automatic statistical electronic voting protocol based on the blockchain[13] designed by McCurry et al. is better to constrain the voting rules.

2.2 Attribute-based Signature(ABS)

So far, attribute-based encryption has spawned many new systems.ABS is mainly divided into three policies: non-monotonic policy, monotonic policy, and threshold-based policy. At the same time, ABS is derived from initial multi-authority ABS[16], traceable ABS[5], linkability ABS[6], etc. Each system has its distinct characteristics, which give unlimited possibilities for encrypted signatures.

2.3 E-petition system

Most of today's e-petition systems are used by government and school departments to collect people's wishes. Some petition systems[14] use statistics on addresses, IP addresses, or email addresses and use multiple layers of encryption to protect people's privacy. 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 due to a failure of the information base. At the same time, there are petitioning systems that combine blockchain and javascript to guarantee that each person can only vote once[15].

3 Syntax of e-Petition system

3.1 System model

As mentioned before, users who have different attributes will sign the different messages, representing different voting numbers. In addition, in Attribute-based Signature, a set $\mathbb{AA} = \{AA_i\}_{i=1}^{n}$ of attribute authorities are established, and $\mathbb{AA}_i$ is the space where attribute authority AA_i manages attributes. Suppose that $\alpha \subset \mathbb{AA}$ is a set of attributes that satisfy a specific predicate, and $a \in \alpha \implies \exists \mathrm{A}_i$, so attribute a belongs to AA_i.

• **Setup** (1^{λ}): This algorithm is executed to set up the whole system. It returns a public parameters pp when input a unary string, which λ is the security parameter.

· Account Establishment: This protocol is executed to establish the user's account. It has three algorism AASetup, UkeyGen, AttKeyGen.

· AASetup(aid,**pp**): Generating public/private key pair($\mathrm{pk}_{AA}, sk_{AA}$) by attribute authority AA_{aid}. The authority keep sk_{AA} privity and release pk_{AA} to the public.

· UkeyGen (id,pp): Generating user's private key sk_{id} by user id.

· AttKeyGen ($f(sk_{id})$,id,a,sk_{AA}): Is run by AA that manages attribute a. AttKeyGen generate the private key skid of user id, and bound id and injective one-way function $f(sk_{id})$.

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

• **Sign** (p, Ω, $sk_{id,\alpha}$,sk_{id}): This algorithm is executed to produce a signature if the user's attributes satisfy the predicate Ω. Users can use corresponding secret keys $sk_{id,\alpha}$ =$\{sk_{id,\alpha_i}\}_{\alpha_i \in \alpha}$ to generate a signature $\sigma = \sigma_{ABS}$ on the petition p.

• **Verify** (σ, $\{\mathrm{pk}_{AA}\}_i$, Ω, p): Take the signature σ on the petition p and verify the signature. The attribute authorities' verification keys $\{pk_{AA_i}\}_i$ manage attributes that are involved in Ω. It will return 1 if the signature is valid.

• **Tally** (verify(), c_{AA_i},$(\mathrm{t}_i)_{(i \in n)}$,MP): This algorithm statistic valid signature, and different attribute authority will has 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.

3.2 Security Model.

The security requirement of an e-petition system is shown as follows.

Anonymity. This require that the signature secret the user's identity and the attributes. We consider the adversary as follows,

·Adversary's Power: The adversary control all attribute. It can take the signer's private key who is chosen. At the same time, it can get any attributes' secret key and it owns a signing oracle which can question messages on behalf of honest users.

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.

·Adversary Power: It owns a signing oracle, and it can ask for user's personal secret key. At the same time, it can corrupt attribute authority and ask for attribute's secret key.

Correctness. Signatures generated by honest users must be properly verified.

3.3 Block model.

Block model. Bilinear Group. A bilinear group is a tuple P =($\mathbb{G}_1$,$\mathbb{G}_2$,$\mathbb{G}_T$,p,g_1,g_2,e), where $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$ are groups of a prime order p, g_1 and g_2 generate $\mathbb{G}_1$ and $\mathbb{G}_2$. [6] We would like use Type-3 in [8] to build our bilinear map $\mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$, which $\mathbb{G}_1 \neq \mathbb{G}_2$, $\mathbb{G}_1$ and $\mathbb{G}_2$ 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/private key pair. We will use a different type of full Boneh-Boyen signature scheme according to [6], namely, BB † scheme. The schemes are described as follows,

· KeyGen(P): Let $x, y \leftarrow \mathbb{Z}_p$, set $(X, Y) = (g_2^x, g_2^y)$, which (X, Y) is the public key and (x, y) is the private key.

· BB.Sign(sk,m): Take the signature $\sigma = g^{1/(x+ry+m)}$ on massage $m \in \mathbb{Z}_p$. In σ, $r \leftarrow \mathbb{Z}_p$ and $x+ry+m \neq 0$. In addition, the signature $\sigma = (g_1 \cdot h_1^z)^{(1/x+ry+m)}$ in BB†.

· Verify: In BB† scheme, if $e(\sigma, X \cdot Y^r \cdot g_2^m) = e(g_1 \cdot h_1^z, g_2)$ 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 [6], 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 $C'= \{y| \exists x, (x, y) \in R\}$. 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 trust this statement 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.

4 Construction of e-petition system

4.1 Overview of construction

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 $(\mathbf{pk_{psdo}}, \mathbf{sk_{prdo}})$ is generated for Digital Signature scheme $\mathbf{D_2}$. At the same time, a public parameter $\mathbf{pp} = (\mathbf{pk_{psdo}}, \mathbf{crs}, \mathbb{A}, \mathcal{H})$, where $\mathcal{H}$ is the collision-resistant hash function.

In account establish algorithm, a public/private key pair$(\mathbf{pk_{aid}}, \mathbf{sk_{aid}})$ is generated for Digital Signature Scheme $\mathbf{D_1}$ after a new attribute authority is created. If the user **id** needs to generate a signing key that the attribute is $a \in \mathbb{A}$,the managing attribute authority the managing attribute authority need to sign **id**, a and one-way function on user's private key $\mathbf{sk_{id}}$ together. This signature is the private key for user's attribute.

Then the user will use this signature to sign the messages that the attributes satisfied. The signature will generate a NIZK proof that the modified predicate Ω' will still has proper user's attribute be satisfied.

According to the [6], the languages for the NIZK proofs are defined as follows. We define a monotone Boolean function $\Phi : \{0, 1\}^n \to 0, 1$, and a matrix in a field F has the size $l \times w$. Then a labelling function make a transition from l to n. If every $(x_1, \ldots, x_n) \in \{0, 1\}^n$, M is a monotone span program for Φ *over* $\mathbb{F}$, *and* v is the secret vector in it, which means,

$[\Phi(x_1, ...x_n) = 1] \Leftrightarrow [\exists v \in \mathbb{F}^{1\times t} : v \cdot M = [1, 0, ..., 0] \bigwedge(\forall i : x_{a(i)} = 0 \Rightarrow v_i = 0)]$

Base on the definition of the span program, the satisfiability of Ω' can be proved. User need to prove the property of the $v \in \mathbb{Z}_p^{|\Omega'|}$ with $v \cdot M = [1, 0, ..., 0]$. The zero element in $v \cdot M$ 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, c_{AA_i} need to count different times base on the petition rule. If Verify $(\sigma, \{pk_{AA}\}_i, \Omega, p) = 1$, then c_{AA_i} will be counted until c_{AA_i} get the maximum number of petitions MP. Then, the algorithm will calculate the ratio of c_{AA_i} to the MP, and output the result.

```
○ Setup(1^λ):
    · $(crs, xk) \leftarrow NIZK.Setup(1^\lambda)$
    · $(\mathbf{pk_{psdo}}, \mathbf{sk_{prdo}}) \leftarrow DS.KeyGen(1^\lambda)$
    · Compute a Collision-resistant hash function $\mathcal{H} : \{0, 1\}^* \to \mathcal{M}_{DS}$
    · $\mathbf{pp} = (\mathbf{pk_{psdo}}, \mathbf{crs}, \mathbb{A}, \mathcal{H})$
    · Return pp
○ Account Establish:
    · $(\mathbf{pk_{aid}}, \mathbf{sk_{aid}}) \leftarrow DS.KeyGen(1^\lambda)$
    · Return $(\mathbf{pk_{aid}}, \mathbf{sk_{aid}})$
    · $sk_{id} \leftarrow$ UKeyGen$(id, pp)$
○ Sign $(p, \Omega, sk_{id,\alpha}, sk_{id})$ :
```

· Return $\perp$ if $\Omega(A) = 0$

· $\Omega' := \Omega \bigvee a_{psdo}, \mathbf{M} \in \mathbb{Z}^{\alpha \times \theta}$ is the Ω' span program.

· Compute $\alpha := \{a_i\}_{i=1}^{|\Omega'|}$ to be the attribute in Ω'

· $\pi \leftarrow NIZK.Prove(crs, x, y)$ if $\mathrm{R}(x, y) = 1$.

· $((\mathbf{pk} = \{pk_i\}_{i=1}^{|\Omega'|}, \mathbf{a} = \{a_i\}_{i=1}^{|\Omega'|}), (\mathrm{sk}_{id}, \mathrm{id}, \mathrm{v}, \boldsymbol{\sigma = \{\sigma_{a_i}\}_{i=1}^{|\Omega'|}})) :$

$(\boldsymbol{v}\mathrm{M}{=}[1,0,...,0]) \bigwedge_{i=1}^{|\Omega'|-1}$

$(v_i = 0 \bigvee \mathrm{D}_1.\mathrm{Verify}(\mathrm{pk}_i, \mathrm{id}, \mathrm{sk}_{id}, \mathrm{a}_i, \sigma_{a_i}){=}1)$

$\bigwedge(\mathrm{v}_{|\Omega'|=0} \bigvee \mathrm{D}_2.\mathrm{Verify}(pk_{psdo}, a_{psdo}, \sigma_{a_{psdo}}){=}1)$

· Return $\sigma{:=}\{\sigma_{a_i}\}_{i=1}^{n}$

○ **Verify** $(\sigma, \{\mathrm{pk}_{AA}\}_i, \Omega, \mathrm{p})$

· Return NIZK.Verify(crs,π)

○ **Tally**(verify(), c_{AA_i},$(\mathrm{t}_{AA_i})_{(i \in n)}$, MP)

· $c_{AA_i} = c_{AA_i} + (t_{AA_i})_{(i \in n)}$ if Verify$(\sigma, \{\mathrm{pk}_{AA}\}_i, \Omega, \mathrm{p}) = 1$

· Return $\sum c_{AA_i}$ if $\sum c_{AA_i}{=}$ MP

· Return $(\frac{c_{AA_i}}{MP})_{i=1}^{n}$

4.2 Detail of construction

User's task in e-petition system is make a zero-knowledge proof of π.

The first step is user need to prove a secret vector v is spanned the public matrix $\mathbf{M}$ which we talked about in span program earlier. The purpose of this step is shown how to hide which subset of user's attributes has used to satisfy the modified predicate Ω' [6]. The Proof process is shown as follows,

$\boldsymbol{v}\mathbf{M}$=[1,0,...,0],which also can be written the following form,

$$\sum_{i=1}^{|\Omega'|} v_i \mathbf{M}_{ij} = \begin{cases} 1 & j = 1 \\ 0 & 2 \leq j \leq \theta \end{cases}$$

· Commitment of v

$$\beta_{v_i}, \beta_{w_i}, w_i \leftarrow \mathbb{Z}_p, i = 1...\alpha$$
$$\overset{\wedge}{v_i} = g_1^{v_i} \cdot k_3^{\beta_{w_i}}$$
$$\mathcal{V}_i = g_1^{\beta_{v_i}} \cdot k_3^{\beta_{w_i}}$$

· Proof of statement

$$\forall j \in [1,\theta]\text{:}\ \Lambda_j = \prod_{i=1}^{\alpha} k_3^{w_i \cdot M_{ij}},\ \lambda_j = \prod_{i=1}^{\alpha} (k_3^{w_i \cdot M_{ij}})^{\beta_{t_i}}$$

The second step is proof whether the signature can be verified base on the verification key.

In Digital Signature, a verification function can be used.

$$e(\sigma_{a_i}^{v_i}, X, Y^r \cdot g_2^{a_i||id}) = e(g_1, g_2) \cdot e(h_1^{sk}, g_2)$$

According to the BB and BB† scheme, the signature can be described as follows,

$$\sigma_{a_i} \begin{cases} (g_1 \cdot h_1^{sk})^{1/x_i + y_i r_i + a_i||id} & attribute \\ (g_1^{1/x_i + y_i r_i + a_{psdo}} & pseudo - attribute \end{cases}$$

The public key of a_i is $X_i = g_2^{x_i}$ and $Y_i = g_2^{y_i}$. We need to replace the zero-element v_i in secret vector v to the random number. The purpose is hide subset of the attributes which satisfied the predicate Ω.

References

[1] Hansard Society. (2010) 'Audit of Political Engagement 7'.

[2] Caygill, Thomas, and Anne-Marie Griffiths. ”Parliament and petitions.” Exploring parliament (2018): 322-332.

[3] Li, Jin, et al. ”Attribute-based signature and its applications.” Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. 2010.

[4] Okamoto T, Takashima K. Decentralized attribute-based signatures. InInternational Workshop on Public Key Cryptography 2013 Feb 26 (pp. 125-142). Springer, Berlin, Heidelberg.

[5] El Kaafarani A, Ghadafi E, Khader D. Decentralized traceable attribute-based signatures. InCryptographers' Track at the RSA Conference 2014 Feb 25 (pp. 327-348). Springer, Cham.

[6] El Kaafarani, Ali, et al. ”Attribute-based signatures with user-controlled linkability.” International Conference on Cryptology and Network Security. Springer, Cham, 2014.

[7] Li, Yannan, et al. ”A blockchain-based self-tallying voting protocol in decentralized IoT.” IEEE Transactions on Dependable and Secure Computing (2020).

[8] Galbraith, Steven D., Kenneth G. Paterson, and Nigel P. Smart. ”Pairings for cryptographers.” Discrete Applied Mathematics 156.16 (2008): 3113-3121.

[9] Zhao, Zhichao, and T-H. Hubert Chan. ”How to vote privately using bitcoin.” International Conference on Information and Communications Security. Springer, Cham, 2015.

[10] Bistarelli, Stefano, et al. ”An end-to-end voting-system based on bitcoin.” Proceedings of the Symposium on Applied Computing. 2017.

[11] Li, Yannan, et al. ”Traceable monero: Anonymous cryptocurrency with enhanced accountability.” IEEE Transactions on Dependable and Secure Computing (2019).

[12] Takabatake, Yu, Daisuke Kotani, and Yasuo Okabe. ”An anonymous distributed electronic voting system using Zerocoin.” IEICE Technical Report 116.282 (2016): 127-131.

[13] McCorry, Patrick, Siamak F. Shahandashti, and Feng Hao. ”A smart contract for boardroom voting with maximum voter privacy.” International Conference on Financial Cryptography and Data Security. Springer, Cham, 2017.

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

[15] Wahab, Jad. ”Coconut E-Petition Implementation.” arXiv preprint arXiv:1809.10956 (2018).

[16] Okamoto, Tatsuaki, and Katsuyuki Takashima. ”Decentralized attribute-based signatures.” International Workshop on Public Key Cryptography. Springer, Berlin, Heidelberg, 2013.