



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0028612
(43) 공개일자 2019년03월19일

(51) 국제특허분류(Int. Cl.)

G06Q 99/00 (2006.01) G06F 21/50 (2013.01)
G06Q 10/10 (2012.01) G06Q 30/02 (2012.01)
G06Q 50/30 (2012.01)

(52) CPC특허분류

G06Q 99/00 (2013.01)
G06F 21/50 (2013.01)

(21) 출원번호 10-2017-0115385

(22) 출원일자 2017년09월08일

심사청구일자 2017년09월08일

(71) 출원인

울산대학교 산학협력단

울산광역시 남구 대학로 93(무거동)

(72) 발명자

이명준

울산광역시 중구 평동3길 1 108동 2001호 (유곡동, 유곡푸르지오아파트)

진재환

울산광역시 남구 두왕로34번길 9-20, 5동 105호 (상개동, 크로바전원빌라아파트)

(뒷면에 계속)

(74) 대리인

특허법인 아이퍼스

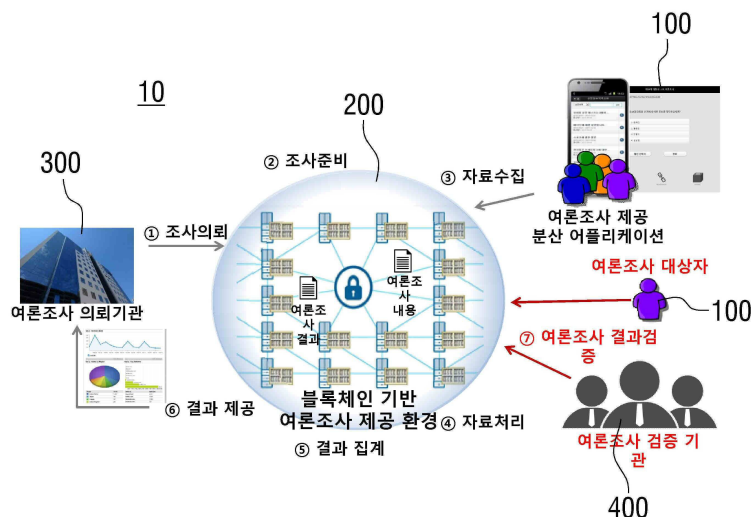
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **블록체인 기반의 여론조사 제공 방법 및 시스템**

(57) 요약

본 발명은 블록체인 기반의 여론조사 제공 방법 및 시스템에 관한 것이다. 본 발명의 일 양상인 블록체인 기반의 조사 방법은, 복수의 서버로 구성된 블록체인 기반의 분산 네트워크가 조사 대상이 되는 적어도 하나의 사용자에게 대한 제 1 정보를 수집하는 제 1 단계; 상기 분산 네트워크가 상기 제 1 정보를 분산시켜 저장하는 제 2 단계; 상기 분산 네트워크가 복수의 사용자 중 상기 분산 네트워크에 저장된 제 1 정보를 통해 인증된 제 1 사용자의 단말로 조사와 관련된 제 2 정보를 전송하는 제 3 단계; 상기 제 2 정보에 대응하여 결정된 제 3 정보가 상기 단말에서 암호화되고, 상기 암호화된 제 3 정보가 상기 분산 네트워크에 전달되는 제 4 단계; 상기 분산 네트워크가 상기 암호화된 제 3 정보를 복호화하여 상기 제 3 정보를 추출하는 제 5 단계; 및 상기 분산 네트워크가 상기 추출한 제 3 정보를 이용하여 상기 조사에 대한 결과를 결정하는 제 6 단계;를 포함할 수 있다.

대표도 - 도5



(52) CPC특허분류

G06Q 10/10 (2013.01)

G06Q 30/0203 (2013.01)

G06Q 50/30 (2015.01)

(72) 발명자

엄현민

울산광역시 동구 안산로 50, (동부동, 현대패밀리동
부아파트) 101동 906호

선주은

부산광역시 해운대구 재송2로 91, 101동 307호(재
송동, 장산동국아파트)

이 발명을 지원한 국가연구개발사업

과제고유번호 2016-0819

부처명 교육부

연구관리전문기관 한국연구재단

연구사업명 지역대학우수과학자지원사업

연구과제명 히스토리 민감형 작업의 효과적 협업을 위한 블록체인 기반의 협업 시스템 개발

기 여 율 1/1

주관기관 울산대학교산학협력단

연구기간 2016.11.01 ~ 2017.10.31

명세서

청구범위

청구항 1

복수의 서버로 구성된 블록체인 기반의 분산 네트워크가 조사 대상이 되는 적어도 하나의 사용자에 대한 제 1 정보를 수집하는 제 1 단계;

상기 분산 네트워크가 상기 제 1 정보를 분산시켜 저장하는 제 2 단계;

상기 분산 네트워크가 복수의 사용자 중 상기 분산 네트워크에 저장된 제 1 정보를 통해 인증된 제 1 사용자의 단말로 조사와 관련된 제 2 정보를 전송하는 제 3 단계;

상기 제 2 정보에 대응하여 결정된 제 3 정보가 상기 단말에서 암호화되고, 상기 암호화된 제 3 정보가 상기 분산 네트워크에 전달되는 제 4 단계;

상기 분산 네트워크가 상기 암호화된 제 3 정보를 복호화하여 상기 제 3 정보를 추출하는 제 5 단계; 및

상기 분산 네트워크가 상기 추출한 제 3 정보를 이용하여 상기 조사에 대한 결과를 결정하는 제 6 단계;를 포함하는 블록체인 기반의 조사 방법.

청구항 2

제 1항에 있어서,

상기 제 6 단계 이후에,

상기 분산 네트워크가 상기 검증 기관으로부터 검증 요청을 수신하는 제 7-1 단계;

상기 분산 네트워크가 상기 암호화된 제 3 정보를 복호화하여 상기 제 3 정보를 추출하고, 상기 추출한 제 3 정보를 이용하여 상기 조사에 대한 제 결과를 결정하는 제 7-2 단계; 및

상기 검증 기관이 상기 분산 네트워크가 수행한 조사에 대한 결과와 상기 제 결과를 비교하여 검증하는 제 7-3 단계;를 더 포함하는 것을 특징으로 하는 블록체인 기반의 조사 방법.

청구항 3

제 1항에 있어서,

상기 제 6 단계 이후에,

상기 인증된 제 1 사용자의 단말이 상기 분산 네트워크로부터 상기 암호화된 제 3 정보를 수신하는 제 8-1 단계;

상기 인증된 제 1 사용자의 단말에서 상기 암호화된 제 3 정보를 복호화하여 상기 제 3 정보를 추출하는 제 8-2 단계; 및

상기 인증된 제 1 사용자의 단말에서 상기 제 1 사용자가 과거에 입력한 정보와 상기 제 3 정보가 일치하는지 여부를 확인하여 검증하는 제 8-3 단계;를 더 포함하는 것을 특징으로 하는 블록체인 기반의 조사 방법.

청구항 4

제 1항에 있어서,

상기 조사는 여론조사이고,

상기 제 2 정보는 복수의 후보를 나타내는 정보이며,

상기 제 3 정보는 상기 복수의 후보 중 적어도 하나의 후보를 지지하는 것을 나타내는 후보인 것을 특징으로 하는 블록체인 기반의 조사 방법.

청구항 5

제 1항에 있어서,

상기 블록체인 기반의 분산 네트워크는 이더리움(Ethereum) 플랫폼 인 것을 특징으로 하는 블록체인 기반의 조사 방법.

청구항 6

조사 대상이 되는 적어도 하나의 사용자에 대한 제 1 정보를 수집하는 복수의 서버로 구성된 블록체인 기반의 분산 네트워크; 및

복수의 사용자 중 상기 분산 네트워크에 저장된 제 1 정보를 통해 인증된 제 1 사용자의 단말;을 포함하되,

상기 분산 네트워크는,

상기 제 1 정보를 분산시켜 저장하고,

상기 제 1 사용자의 단말로 조사와 관련된 제 2 정보를 전송하며,

상기 제 2 정보에 대응하여 결정된 제 3 정보가 상기 단말에서 암호화되고, 상기 암호화된 제 3 정보가 상기 분산 네트워크에 전달되는 경우,

상기 분산 네트워크는,

상기 암호화된 제 3 정보를 복호화하여 상기 제 3 정보를 추출하고,

상기 추출한 제 3 정보를 이용하여 상기 조사에 대한 결과를 결정하는 것을 특징으로 하는 블록체인 기반의 조사 시스템.

청구항 7

제 6항에 있어서,

상기 분산 네트워크가 검증 기관으로부터 검증 요청을 수신하는 경우,

상기 분산 네트워크는,

상기 암호화된 제 3 정보를 복호화하여 상기 제 3 정보를 추출하고, 상기 추출한 제 3 정보를 이용하여 상기 조사에 대한 제 결과를 결정하며,

상기 분산 네트워크가 수행한 조사에 대한 결과와 상기 제 결과를 비교하여 검증하는 것을 특징으로 하는 블록체인 기반의 조사 시스템.

청구항 8

제 6항에 있어서,

상기 인증된 제 1 사용자의 단말은,

상기 분산 네트워크로부터 상기 암호화된 제 3 정보를 수신하고,

상기 암호화된 제 3 정보를 복호화하여 상기 제 3 정보를 추출하며,

상기 제 1 사용자가 과거에 입력한 정보와 상기 제 3 정보가 일치하는지 여부를 확인하여 검증하는 것을 특징으로 하는 블록체인 기반의 조사 시스템.

청구항 9

제 6항에 있어서,

상기 조사는 여론조사이고,

상기 제 2 정보는 복수의 후보를 나타내는 정보이며,

상기 제 3 정보는 상기 복수의 후보 중 적어도 하나의 후보를 지지하는 것을 나타내는 후보인 것을 특징으로 하

는 블록체인 기반의 조사 시스템.

청구항 10

제 6항에 있어서,

상기 블록체인 기반의 분산 네트워크는 이더리움(Ethereum) 플랫폼 인 것을 특징으로 하는 블록체인 기반의 조사 시스템.

발명의 설명

기술 분야

- [0001] 본 발명은 블록체인 기반의 여론조사 제공 방법 및 시스템에 관한 것이다. 구체적으로, 본 발명은 신뢰성을 보장하는 블록체인 기반의 여론조사 제공 기법 및 투표 검증 기법에 관한 것으로, 블록체인 기반의 이더리움 플랫폼 환경에서 여론조사의 생성에서부터 대상자의 관리, 투표 수행 등 기본적인 여론조사를 수행함과 동시에 개인이나 인증 기관을 통한 여론조사 결과의 검증 기능을 제안하고 있다.

배경 기술

- [0002] 여론조사는 특정 사회 집단의 여론을 알아보는 수단으로서 여론조사 기관에서 제공하는 여론조사지를 통해 대상자들의 문항별 투표를 수집하여 결과를 도출하는데, 여론조사의 결과는 해당 문항들에 대한 다수 여론의 성향을 나타내는 것이므로 여러 기관이나 시스템에서의 그 활용 가치가 매우 높다.
- [0003] 이로 인해 여론조사에 대한 위변조의 문제점이 고려되며 조사결과에 대한 신뢰성 보장이 중요한 이슈로 발생되고, 최근에는 위변조가 불가능한 분산 장부 관리 기법인 블록체인을 기반으로 신뢰성이 보장되는 투표 방법에 대한 연구가 등장하고 있다.
- [0004] 그러나 종래의 방법은 투표에 대한 기본적인 기능만을 제공하므로 다양한 문항으로 구성된 여론조사에 활용하기는 어려움이 있으며 더욱 신뢰성 있는 결과를 위한 투표결과 검증 서비스를 지원할 수 없다.
- [0005] 따라서 상기 문제점을 해소하기 위해 블록체인을 이용하여 안전하게 결과 값을 저장하면서도 매우 간단하게 결과 값을 검증함으로써, 여론조사에 대한 효율성과 신뢰성을 높이기 위한 해결방법에 대한 요구가 높아지고 있는 실정이다.

선행기술문헌

특허문헌

- [0006] (특허문헌 0001) 대한민국 특허청 등록번호 제10-1205385호
(특허문헌 0002) 국제출원번호 PCT/US2009/038901

발명의 내용

해결하려는 과제

- [0007] 본 발명은 블록체인 기반의 여론조사 제공 방법 및 시스템을 사용자에게 제공하고자 한다.
- [0008] 구체적으로, 본 발명은 신뢰성을 보장하는 블록체인 기반의 여론조사 제공 기법 및 투표 검증 기법에 관한 것으로, 블록체인 기반의 이더리움 플랫폼 환경에서 여론조사의 생성에서부터 대상자의 관리, 투표 수행 등 기본적인 여론조사를 수행함과 동시에 개인이나 인증 기관을 통한 여론조사 결과의 검증 기능을 제안하고자 한다.
- [0009] 한편, 본 발명에서 이루고자 하는 기술적 과제들은 이상에서 언급한 기술적 과제들로 제한되지 않으며, 언급하지 않은 또 다른 기술적 과제들은 아래의 기재로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

- [0010] 상기의 기술적 과제를 달성하기 위한 본 발명의 일 양상인 블록체인 기반의 조사 방법은, 복수의 서버로 구성된 블록체인 기반의 분산 네트워크가 조사 대상이 되는 적어도 하나의 사용자에게 대한 제 1 정보를 수집하는 제 1 단계; 상기 분산 네트워크가 상기 제 1 정보를 분산시켜 저장하는 제 2 단계; 상기 분산 네트워크가 복수의 사용자 중 상기 분산 네트워크에 저장된 제 1 정보를 통해 인증된 제 1 사용자의 단말로 조사와 관련된 제 2 정보를 전송하는 제 3 단계; 상기 제 2 정보에 대응하여 결정된 제 3 정보가 상기 단말에서 암호화되고, 상기 암호화된 제 3 정보가 상기 분산 네트워크에 전달되는 제 4 단계; 상기 분산 네트워크가 상기 암호화된 제 3 정보를 복호화하여 상기 제 3 정보를 추출하는 제 5 단계; 및 상기 분산 네트워크가 상기 추출한 제 3 정보를 이용하여 상기 조사에 대한 결과를 결정하는 제 6 단계;를 포함할 수 있다.
- [0011] 또한, 상기 제 6 단계 이후에, 상기 분산 네트워크가 상기 검증 기관으로부터 검증 요청을 수신하는 제 7-1 단계; 상기 분산 네트워크가 상기 암호화된 제 3 정보를 복호화하여 상기 제 3 정보를 추출하고, 상기 추출한 제 3 정보를 이용하여 상기 조사에 대한 제 결과를 결정하는 제 7-2 단계; 및 상기 검증 기관이 상기 분산 네트워크가 수행한 조사에 대한 결과와 상기 제 결과를 비교하여 검증하는 제 7-3 단계;를 더 포함할 수 있다.
- [0012] 또한, 상기 제 6 단계 이후에, 상기 인증된 제 1 사용자의 단말이 상기 분산 네트워크로부터 상기 암호화된 제 3 정보를 수신하는 제 8-1 단계; 상기 인증된 제 1 사용자의 단말에서 상기 암호화된 제 3 정보를 복호화하여 상기 제 3 정보를 추출하는 제 8-2 단계; 상기 인증된 제 1 사용자의 단말에서 상기 제 1 사용자가 과거에 입력한 정보와 상기 제 3 정보가 일치하는지 여부를 확인하여 검증하는 제 8-3 단계;를 더 포함할 수 있다.
- [0013] 또한, 상기 조사는 여론조사이고, 상기 제 2 정보는 복수의 후보를 나타내는 정보이며, 상기 제 3 정보는 상기 복수의 후보 중 적어도 하나의 후보를 지지하는 것을 나타내는 후보일 수 있다.
- [0014] 또한, 상기 블록체인 기반의 분산 네트워크는 이더리움(Ethereum) 플랫폼 일 수 있다.
- [0015] 한편, 상기의 기술적 과제를 달성하기 위한 본 발명의 다른 양상인 블록체인 기반의 조사 시스템은, 조사 대상이 되는 적어도 하나의 사용자에게 대한 제 1 정보를 수집하는 복수의 서버로 구성된 블록체인 기반의 분산 네트워크; 및 복수의 사용자 중 상기 분산 네트워크에 저장된 제 1 정보를 통해 인증된 제 1 사용자의 단말;을 포함하되, 상기 분산 네트워크는, 상기 제 1 정보를 분산시켜 저장하고, 상기 제 1 사용자의 단말로 조사와 관련된 제 2 정보를 전송하며, 상기 제 2 정보에 대응하여 결정된 제 3 정보가 상기 단말에서 암호화되고, 상기 암호화된 제 3 정보가 상기 분산 네트워크에 전달되는 경우, 상기 분산 네트워크는, 상기 암호화된 제 3 정보를 복호화하여 상기 제 3 정보를 추출하고, 상기 추출한 제 3 정보를 이용하여 상기 조사에 대한 결과를 결정할 수 있다.
- [0016] 또한, 상기 분산 네트워크가 검증 기관으로부터 검증 요청을 수신하는 경우, 상기 분산 네트워크는, 상기 암호화된 제 3 정보를 복호화하여 상기 제 3 정보를 추출하고, 상기 추출한 제 3 정보를 이용하여 상기 조사에 대한 제 결과를 결정하며, 상기 분산 네트워크가 수행한 조사에 대한 결과와 상기 제 결과를 비교하여 검증할 수 있다.
- [0017] 또한, 상기 인증된 제 1 사용자의 단말은, 상기 분산 네트워크로부터 상기 암호화된 제 3 정보를 수신하고, 상기 암호화된 제 3 정보를 복호화하여 상기 제 3 정보를 추출하며, 상기 제 1 사용자가 과거에 입력한 정보와 상기 제 3 정보가 일치하는지 여부를 확인하여 검증할 수 있다.
- [0018] 또한, 상기 조사는 여론조사이고, 상기 제 2 정보는 복수의 후보를 나타내는 정보이며, 상기 제 3 정보는 상기 복수의 후보 중 적어도 하나의 후보를 지지하는 것을 나타내는 후보일 수 있다.
- [0019] 또한, 상기 블록체인 기반의 분산 네트워크는 이더리움(Ethereum) 플랫폼 일 수 있다.

발명의 효과

- [0020] 본 발명은 블록체인 기반의 여론조사 제공 방법 및 시스템을 사용자에게 제공하고자 할 수 있다.
- [0021] 구체적으로, 본 발명은 신뢰성을 보장하는 블록체인 기반의 여론조사 제공 기법 및 투표 검증 기법에 관한 것으로, 블록체인 기반의 이더리움 플랫폼 환경에서 여론조사의 생성에서부터 대상자의 관리, 투표 수행 등 기본적인 여론조사를 수행함과 동시에 개인이나 인증 기관을 통한 여론조사 결과의 검증 기능을 제안하고자 할 수 있다.
- [0022] 본 발명이 제안하는 여론조사 제공 기법은 상기 문제점을 해소하기 위해 블록체인을 이용하여 안전하게 결과 값을 저장하면서도 매우 간단하게 결과 값을 검증할 수 있다는 점에서 여론조사에 대한 효율성과 신뢰성을 높이기

위한 해결방법으로 활용될 수 있을 것으로 판단되므로, 높은 시장성을 보유하고 있다.

[0023] 한편, 본 발명에서 이루고자 하는 기술적 과제들은 이상에서 언급한 기술적 과제들로 제한되지 않으며, 언급하지 않은 또 다른 기술적 과제들은 아래의 기재로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

[0024] 다만, 본 발명에서 얻을 수 있는 효과는 이상에서 언급한 효과들로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0025] 도 1은 본 발명에 적용되는 단말을 설명하기 위한 블록 구성도이다.

도 2는 도 1에서 설명한 단말을 기초로 제공되는 여론조사 시스템의 일례를 설명하는 블록 구성도이다.

도 3은 종래의 방식에 따른 여론조사 시스템의 일례를 설명하는 도면이다.

도 4는 본 발명이 제안하는 블록체인 기반의 여론조사에서 여론조사 스마트 컨트랙트 구조를 설명하기 위한 도면이다.

도 5는 본 발명이 제안하는 블록체인 기반의 여론조사 시스템 개념도의 일례를 도시한 것이다.

도 6은 도 5에서 설명한 블록체인 기반의 여론조사 시스템이 여론조사 생성, 관리 및 여론조사를 수행하는 과정을 설명한 것이다.

도 7은 도 6에서 설명한 여론조사 생성 과정을 보다 자세하게 설명한 액티비티 다이어그램의 일례이다.

도 8은 도 5에서 설명한 블록체인 기반의 여론조사 시스템이 여론조사결과를 검증하는 과정을 설명한 것이다.

도 9는 도 8에서 설명한 여론조사 검증 과정을 보다 자세하게 설명한 액티비티 다이어그램의 일례를 도시한 것이다.

도 10은 본 발명이 제안하는 시스템 중 여론조사 투표데이터의 암호화 및 복호화 과정을 설명하기 위한 도면이다.

도 11a는 종래의 기존 공개키/비밀키 암호화 방법을 설명한 도면이고, 도 11b는 본 발명이 제안하는 투표데이터의 암호화 및 복호화 과정을 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0026] 본 발명이 제안하는 방법을 설명하기에 앞서, 여론조사 대상인 사용자들이 사용하는 기기인 단말(100)에 대해 구체적으로 설명한다.

[0027] 도 1은 본 발명에 적용되는 단말을 설명하기 위한 블록 구성도이다.

[0028] 도 1을 참조하면, 단말(100)는 무선 통신부(110), A/V(Audio/Video) 입력부(120), 사용자 입력부(130), 센싱부(140), 출력부(150), 메모리(160), 인터페이스부(170), 제어부(180) 및 전원 공급부(190) 등을 포함할 수 있다.

[0029] 단, 도 1에 도시된 구성요소들이 필수적인 것은 아니어서, 그보다 많은 구성요소들을 갖거나 그보다 적은 구성요소들을 갖는 단말이 구현될 수도 있다.

[0030] 이하, 상기 구성요소들에 대해 차례로 살펴본다.

[0031] 무선 통신부(110)는 단말과 무선 통신 시스템 사이 또는 기기와 기기가 위치한 네트워크 사이의 무선 통신을 가능하게 하는 하나 이상의 모듈을 포함할 수 있다.

[0032] 예를 들어, 무선 통신부(110)는 방송 수신 모듈(111), 이동통신 모듈(112), 무선 인터넷 모듈(113), 근거리 통신 모듈(114) 및 위치정보 모듈(115) 등을 포함할 수 있다.

[0033] 방송 수신 모듈(111)은 방송 채널을 통하여 외부의 방송 관리 서버로부터 방송 신호 및/또는 방송 관련된 정보를 수신한다.

- [0034] 상기 방송 채널은 위성 채널, 지상파 채널을 포함할 수 있다. 상기 방송 관리 서버는, 방송 신호 및/또는 방송 관련 정보를 생성하여 송신하는 서버 또는 기 생성된 방송 신호 및/또는 방송 관련 정보를 제공받아 단말에 송신하는 서버를 의미할 수 있다. 상기 방송 신호는, TV 방송 신호, 라디오 방송 신호, 데이터 방송 신호를 포함할 뿐만 아니라, TV 방송 신호 또는 라디오 방송 신호에 데이터 방송 신호가 결합한 형태의 방송 신호도 포함할 수 있다.
- [0035] 상기 방송 관련 정보는, 방송 채널, 방송 프로그램 또는 방송 서비스 제공자에 관련한 정보를 의미할 수 있다. 상기 방송 관련 정보는, 이동통신망을 통하여도 제공될 수 있다. 이러한 경우에는 상기 이동통신 모듈(112)에 의해 수신될 수 있다.
- [0036] 상기 방송 관련 정보는 다양한 형태로 존재할 수 있다. 예를 들어, DMB(Digital Multimedia Broadcasting)의 EPG(Electronic Program Guide) 또는 DVB-H(Digital Video Broadcast-Handheld)의 ESG(Electronic Service Guide) 등의 형태로 존재할 수 있다.
- [0037] 상기 방송 수신 모듈(111)은, 예를 들어, DMB-T(Digital Multimedia Broadcasting-Terrestrial), DMB-S(Digital Multimedia Broadcasting-Satellite), MediaFLO(Media Forward Link Only), DVB-H(Digital Video Broadcast-Handheld), ISDB-T(Integrated Services Digital Broadcast-Terrestrial) 등의 디지털 방송 시스템을 이용하여 디지털 방송 신호를 수신할 수 있다. 물론, 상기 방송 수신 모듈(111)은, 상술한 디지털 방송 시스템뿐만 아니라 다른 방송 시스템에 적합하도록 구성될 수도 있다.
- [0038] 방송 수신 모듈(111)을 통해 수신된 방송 신호 및/또는 방송 관련 정보는 메모리(160)에 저장될 수 있다.
- [0039] 이동통신 모듈(112)은, 이동 통신망 상에서 기지국, 외부의 기기, 서버 중 적어도 하나와 무선 신호를 송수신한다.
- [0040] 문자/멀티미디어 메시지 송수신에 따른 다양한 형태의 데이터를 포함할 수 있다.
- [0041] 무선 인터넷 모듈(113)은 무선 인터넷 접속을 위한 모듈을 말하는 것으로, 단말에 내장되거나 외장될 수 있다. 무선 인터넷 기술로는 WLAN(Wireless LAN)(Wi-Fi), Wibro(Wireless broadband), Wimax(World Interoperability for Microwave Access), HSDPA(High Speed Downlink Packet Access) 등이 이용될 수 있다.
- [0042] 근거리 통신 모듈(114)은 근거리 통신을 위한 모듈을 말한다. 근거리 통신(short range communication) 기술로 블루투스(Bluetooth), RFID(Radio Frequency Identification), 적외선 통신(IrDA, infrared Data Association), UWB(Ultra Wideband), ZigBee, 와이파이(Wireless Fidelity, Wi-Fi) 등이 이용될 수 있다.
- [0043] 위치정보 모듈(115)은 단말의 위치를 획득하기 위한 모듈로서, 그의 대표적인 예로는 GPS(Global Position System) 모듈이 있다.
- [0044] 도 1을 참조하면, A/V(Audio/Video) 입력부(120)는 오디오 신호 또는 비디오 신호 입력을 위한 것으로, 이에는 카메라(121)와 마이크(122) 등이 포함될 수 있다. 카메라(121)는 촬영 모드에서 이미지 센서에 의해 얻어지는 정지영상 또는 동영상 등의 화상 프레임을 처리한다. 처리된 화상 프레임은 디스플레이부(151)에 표시될 수 있다.
- [0045] 카메라(121)에서 처리된 화상 프레임은 메모리(160)에 저장되거나 무선 통신부(110)를 통하여 외부로 전송될 수 있다. 카메라(121)는 사용 환경에 따라 2개 이상이 구비될 수도 있다.
- [0046] 마이크(122)는 녹음모드, 음성인식 모드 등에서 마이크로폰(Microphone)에 의해 외부의 음향 신호를 입력받아 전기적인 음성 데이터로 처리한다. 처리된 음성 데이터는 이동통신 모듈(112)을 통하여 이동통신 기지국으로 송신 가능한 형태로 변환되어 출력될 수 있다. 마이크(122)에는 외부의 음향 신호를 입력받는 과정에서 발생하는 잡음(noise)을 제거하기 위한 다양한 잡음 제거 알고리즘이 구현될 수 있다.
- [0047] 사용자 입력부(130)는 사용자가 단말의 동작 제어를 위한 입력 데이터를 발생시킨다. 사용자 입력부(130)는 키 패드(key pad) 돔 스위치 (dome switch), 터치 패드(정압/정전), 조그 휠, 조그 스위치 등으로 구성될 수 있다.
- [0048] 센싱부(140)는 단말의 개폐 상태, 단말의 위치, 사용자 접촉 유무, 단말의 방위, 단말의 가속/감속 등과 같이 단말의 현 상태를 감지하여 단말의 동작을 제어하기 위한 센싱 신호를 발생시킨다.
- [0049] 센싱부(140)는 전원 공급부(190)의 전원 공급 여부, 인터페이스부(170)의 외부 기기 결합 여부 등을 센싱할 수도 있다.

- [0050] 한편, 상기 센싱부(140)는 근접 센서(141)를 포함할 수 있다.
- [0051] 또한, 센싱부(140)는 초음파 센서(142)를 더 포함할 수 있다.
- [0052] 초음파 센서(142)는 사람의 귀에 들리지 않을 정도로 높은 주파수(약 20 KHz 이상)의 소리인 초음파가 가지고 있는 특성을 이용한 센서를 말한다.
- [0053] 초음파는 공기나 액체, 고체에 사용할 수 있다. 주파수가 높고 파장이 짧기 때문에 높은 분해력을 계측할 수 있는 특징이 있다.
- [0054] 초음파 센서(142)에 이용되는 파장은 매체의 음속과 음파의 주파수에 따라 결정되고, 바다 속의 어군탐지기나 소나에서는 1mm~100mm, 금속 탐상 등에서는 0.5mm~15mm, 기체 속에서는 5~35mm 정도이다.
- [0055] 초음파 센서(142)는 초음파의 발신소자와 수신소자가 동일하고, 센서 재료로는 자기변형 재료(페라이트 등)나 전압, 전기 변형재료(로셀염, 티탄산 바륨 등)가 이용되고 있다.
- [0056] 출력부(150)는 시각, 청각 또는 촉각 등과 관련된 출력을 발생시키기 위한 것으로, 이에 디스플레이부(151), 음향 출력 모듈(152), 알람부(153), 햅틱 모듈(154) 및 프로젝터 모듈(155) 등이 포함될 수 있다.
- [0057] 디스플레이부(151)는 단말에서 처리되는 정보를 표시(출력)한다.
- [0058] 디스플레이부(151)는 액정 디스플레이(liquid crystal display, LCD), 박막 트랜지스터 액정 디스플레이(thin film transistor-liquid crystal display, TFT LCD), 유기 발광 다이오드(organic light-emitting diode, OLED), 플렉시블 디스플레이(flexible display), 3차원 디스플레이(3D display) 중에서 적어도 하나를 포함할 수 있다.
- [0059] 이들 중 일부 디스플레이는 그를 통해 외부를 볼 수 있도록 투명형 또는 광투과형으로 구성될 수 있다. 이는 투명 디스플레이라 호칭될 수 있는데, 상기 투명 디스플레이의 대표적인 예로는 TOLED(Transparent OLED) 등이 있다. 디스플레이부(151)의 후방 구조 또한 광 투과형 구조로 구성될 수 있다. 이러한 구조에 의하여, 사용자는 단말 바디의 디스플레이부(151)가 차지하는 영역을 통해 단말 바디의 후방에 위치한 사물을 볼 수 있다.
- [0060] 단말의 구현 형태에 따라 디스플레이부(151)이 2개 이상 존재할 수 있다. 예를 들어, 단말에는 복수의 디스플레이부들이 하나의 면에 이격되거나 일체로 배치될 수 있고, 또한 서로 다른 면에 각각 배치될 수도 있다.
- [0061] 디스플레이부(151)와 터치 동작을 감지하는 센서(이하, '터치 센서'라 함)가 상호 레이어 구조를 이루는 경우(이하, '터치 스크린'이라 함)에, 디스플레이부(151)는 출력 장치 이외에 입력 장치로도 사용될 수 있다. 터치 센서는, 예를 들어, 터치 필름, 터치 시트, 터치 패드 등의 형태를 가질 수 있다.
- [0062] 터치 센서는 디스플레이부(151)의 특정 부위에 가해진 압력 또는 디스플레이부(151)의 특정 부위에 발생하는 정전 용량 등의 변화를 전기적인 입력신호로 변환하도록 구성될 수 있다. 터치 센서는 터치 되는 위치 및 면적뿐만 아니라, 터치 시의 압력까지도 검출할 수 있도록 구성될 수 있다.
- [0063] 터치 센서에 대한 터치 입력이 있는 경우, 그에 대응하는 신호(들)는 터치 제어기로 보내진다. 터치 제어기는 그 신호(들)를 처리한 다음 대응하는 데이터를 제어부(180)로 전송한다. 이로써, 제어부(180)는 디스플레이부(151)의 어느 영역이 터치 되었는지 여부 등을 알 수 있게 된다.
- [0064] 상기 근접 센서(141)는 상기 터치스크린에 의해 감싸지는 단말의 내부 영역 또는 상기 터치 스크린의 근처에 배치될 수 있다. 상기 근접 센서는 소정의 검출면에 접근하는 물체, 혹은 근방에 존재하는 물체의 유무를 전자계의 힘 또는 적외선을 이용하여 기계적 접촉이 없이 검출하는 센서를 말한다. 근접 센서는 접촉식 센서보다는 그 수명이 길며 그 활용도 또한 높다.
- [0065] 상기 근접 센서의 예로는 투과형 광전 센서, 직접 반사형 광전 센서, 미러 반사형 광전 센서, 고주파 발진형 근접 센서, 정전용량형 근접 센서, 자기형 근접 센서, 적외선 근접 센서 등이 있다. 상기 터치스크린이 정전식인 경우에는 상기 포인터의 근접에 따른 전기장의 변화로 상기 포인터의 근접을 검출하도록 구성된다. 이 경우 상기 터치 스크린(터치 센서)은 근접 센서로 분류될 수도 있다.
- [0066] 이하에서는 설명의 편의를 위해, 상기 터치스크린 상에 포인터가 접촉되지 않으면서 근접되어 상기 포인터가 상기 터치스크린 상에 위치함이 인식되도록 하는 행위를 "근접 터치(proximity touch)"라고 칭하고, 상기 터치스크린 상에 포인터가 실제로 접촉되는 행위를 "접촉 터치(contact touch)"라고 칭한다. 상기 터치스크린 상에서 포인터로 근접 터치가 되는 위치라 함은, 상기 포인터가 근접 터치될 때 상기 포인터가 상기 터치스크린에 대해

수직으로 대응되는 위치를 의미한다.

- [0067] 상기 근접센서는, 근접 터치와, 근접 터치 패턴(예를 들어, 근접 터치 거리, 근접 터치 방향, 근접 터치 속도, 근접 터치 시간, 근접 터치 위치, 근접 터치 이동 상태 등)을 감지한다. 상기 감지된 근접 터치 동작 및 근접 터치 패턴에 상응하는 정보는 터치 스크린상에 출력될 수 있다.
- [0068] 음향 출력 모듈(152)은 녹음 모드, 음성인식 모드, 방송수신 모드 등에서 무선 통신부(110)로부터 수신되거나 메모리(160)에 저장된 오디오 데이터를 출력할 수 있다. 음향 출력 모듈(152)은 단말에서 수행되는 기능과 관련된 음향 신호를 출력하기도 한다. 이러한 음향 출력 모듈(152)에는 리시버(Receiver), 스피커(speaker), 버저(Buzzer) 등이 포함될 수 있다.
- [0069] 알람부(153)는 단말의 이벤트 발생을 알리기 위한 신호를 출력한다.
- [0070] 알람부(153)는 비디오 신호나 오디오 신호 이외에 다른 형태, 예를 들어 진동으로 이벤트 발생을 알리기 위한 신호를 출력할 수도 있다.
- [0071] 상기 비디오 신호나 오디오 신호는 디스플레이부(151)나 음성 출력 모듈(152)을 통해서도 출력될 수 있어서, 그들(151, 152)은 알람부(153)의 일부로 분류될 수도 있다.
- [0072] 햅틱 모듈(haptic module)(154)은 사용자가 느낄 수 있는 다양한 촉각 효과를 발생시킨다. 햅틱 모듈(154)이 발생시키는 촉각 효과의 대표적인 예로는 진동이 있다. 햅틱 모듈(154)이 발생하는 진동의 세기와 패턴 등은 제어 가능하다.
- [0073] 예를 들어, 서로 다른 진동을 합성하여 출력하거나 순차적으로 출력할 수도 있다.
- [0074] 햅틱 모듈(154)은, 진동 외에도, 접촉 피부면에 대해 수직 운동하는 핀 배열, 분사구나 흡입구를 통한 공기의 분사력이나 흡입력, 피부 표면에 대한 스침, 전극(electrode)의 접촉, 정전기력 등의 자극에 의한 효과와, 흡열이나 발열 가능한 소자를 이용한 냉온감 재현에 의한 효과 등 다양한 촉각 효과를 발생시킬 수 있다.
- [0075] 햅틱 모듈(154)은 직접적인 접촉을 통해 촉각 효과의 전달할 수 있을 뿐만 아니라, 사용자가 손가락이나 팔 등의 근 감각을 통해 촉각 효과를 느낄 수 있도록 구현할 수도 있다. 햅틱 모듈(154)은 단말의 구성 태양에 따라 2개 이상이 구비될 수 있다.
- [0076] 프로젝터 모듈(155)은, 단말을 이용하여 이미지 프로젝트(project) 기능을 수행하기 위한 구성요소로서, 제어부(180)의 제어 신호에 따라 디스플레이부(151)상에 디스플레이되는 영상과 동일하거나 적어도 일부가 다른 영상을 외부 스크린 또는 벽에 디스플레이할 수 있다.
- [0077] 구체적으로, 프로젝터 모듈(155)은, 영상을 외부로 출력하기 위한 빛(일 예로서, 레이저 광)을 발생시키는 광원(미도시), 광원에 의해 발생한 빛을 이용하여 외부로 출력할 영상을 생성하기 위한 영상 생성 수단(미도시), 및 영상을 일정 초점 거리에서 외부로 확대 출력하기 위한 렌즈(미도시)를 포함할 수 있다. 또한, 프로젝터 모듈(155)은, 렌즈 또는 모듈 전체를 기계적으로 움직여 영상 투사 방향을 조절할 수 있는 장치(미도시)를 포함할 수 있다.
- [0078] 프로젝터 모듈(155)은 디스플레이 수단의 소자 종류에 따라 CRT(Cathode Ray Tube) 모듈, LCD(Liquid Crystal Display) 모듈 및 DLP(Digital Light Processing) 모듈 등으로 나뉠 수 있다. 특히, DLP 모듈은, 광원에서 발생한 빛이 DMD(Digital Micromirror Device) 칩에 반사됨으로써 생성된 영상을 확대 투사하는 방식으로 프로젝터 모듈(151)의 소형화에 유리할 수 있다.
- [0079] 바람직하게, 프로젝터 모듈(155)은, 단말의 측면, 정면 또는 배면에 길이 방향으로 구비될 수 있다. 물론, 프로젝터 모듈(155)은, 필요에 따라 단말의 어느 위치여라도 구비될 수 있음은 당연하다.
- [0080] 메모리부(160)는 제어부(180)의 처리 및 제어를 위한 프로그램이 저장될 수도 있고, 입/출력되는 데이터들(예를 들어, 메시지, 오디오, 정지영상, 동영상 등)의 임시 저장을 위한 기능을 수행할 수도 있다. 상기 메모리부(160)에는 상기 데이터들 각각에 대한 사용 빈도도 함께 저장될 수 있다. 또한, 상기 메모리부(160)에는 상기 터치스크린 상의 터치 입력시 출력되는 다양한 패턴의 진동 및 음향에 관한 데이터를 저장할 수 있다.
- [0081] 메모리(160)는 플래시 메모리 타입(flash memory type), 하드디스크 타입(hard disk type), 멀티미디어 카드 마이크로 타입(multimedia card micro type), 카드 타입의 메모리(예를 들어 SD 또는 XD 메모리 등), 램(Random Access Memory, RAM), SRAM(Static Random Access Memory), 롬(Read-Only Memory, ROM),

EEPROM(Electrically Erasable Programmable Read-Only Memory), PROM(Programmable Read-Only Memory), 자기 메모리, 자기 디스크, 광디스크 중 적어도 하나의 타입의 저장매체를 포함할 수 있다. 단말은 인터넷(internet)상에서 상기 메모리(160)의 저장 기능을 수행하는 웹 스토리지(web storage)와 관련되어 동작할 수도 있다.

- [0082] 인터페이스부(170)는 단말에 연결되는 모든 외부기기와의 통로 역할을 한다. 인터페이스부(170)는 외부 기기로부터 데이터를 전송받거나, 전원을 공급받아 단말 내부의 각 구성 요소에 전달하거나, 단말 내부의 데이터가 외부 기기로 전송되도록 한다. 예를 들어, 유/무선 헤드셋 포트, 외부 충전기 포트, 유/무선 데이터 포트, 메모리 카드(memory card) 포트, 식별 모듈이 구비된 장치를 연결하는 포트, 오디오 I/O(Input/Output) 포트, 비디오 I/O(Input/Output) 포트, 이어폰 포트 등이 인터페이스부(170)에 포함될 수 있다.
- [0083] 식별 모듈은 단말의 사용 권한을 인증하기 위한 각종 정보를 저장한 칩으로서, 사용자 인증 모듈(User Identify Module, UIM), 가입자 인증 모듈(Subscriber Identify Module, SIM), 범용 사용자 인증 모듈(Universal Subscriber Identity Module, USIM) 등을 포함할 수 있다. 식별 모듈이 구비된 장치(이하 '식별 장치')는, 스마트 카드(smart card) 형식으로 제작될 수 있다. 따라서 식별 장치는 포트를 통하여 단말과 연결될 수 있다.
- [0084] 상기 인터페이스부는 단말이 외부 크래들(cradle)과 연결될 때 상기 크래들로부터의 전원이 상기 단말에 공급되는 통로가 되거나, 사용자에 의해 상기 크래들에서 입력되는 각종 명령 신호가 상기 이동기기로 전달되는 통로가 될 수 있다. 상기 크래들로부터 입력되는 각종 명령 신호 또는 상기 전원은 상기 이동기기가 상기 크래들에 정확히 장착되었음을 인지하기 위한 신호로 동작될 수도 있다.
- [0085] 제어부(controller, 180)는 통상적으로 단말의 전반적인 동작을 제어한다.
- [0086] 제어부(180)는 멀티 미디어 재생을 위한 멀티미디어 모듈(181)을 구비할 수도 있다. 멀티미디어 모듈(181)은 제어부(180) 내에 구현될 수도 있고, 제어부(180)와 별도로 구현될 수도 있다.
- [0087] 상기 제어부(180)는 상기 터치스크린 상에서 행해지는 필기 입력 또는 그림 그리기 입력을 각각 문자 및 이미지로 인식할 수 있는 패턴 인식 처리를 행할 수 있다.
- [0088] 전원 공급부(190)는 제어부(180)의 제어에 의해 외부의 전원, 내부의 전원을 인가 받아 각 구성요소들의 동작에 필요한 전원을 공급한다.
- [0089] 여기에 설명되는 다양한 실시예는 예를 들어, 소프트웨어, 하드웨어 또는 이들의 조합된 것을 이용하여 컴퓨터 또는 이와 유사한 장치로 읽을 수 있는 기록매체 내에서 구현될 수 있다.
- [0090] 하드웨어적인 구현에 의하면, 여기에 설명되는 실시예는 ASICs (application specific integrated circuits), DSPs (digital signal processors), DSPDs (digital signal processing devices), PLDs (programmable logic devices), FPGAs (field programmable gate arrays, 프로세서(processors), 제어기(controllers), 마이크로 컨트롤러(micro-controllers), 마이크로 프로세서(microprocessors), 기타 기능 수행을 위한 전기적인 유닛 중 적어도 하나를 이용하여 구현될 수 있다. 일부의 경우에 본 명세서에서 설명되는 실시예들이 제어부(180) 자체로 구현될 수 있다.
- [0091] 소프트웨어적인 구현에 의하면, 본 명세서에서 설명되는 절차 및 기능과 같은 실시예들은 별도의 소프트웨어 모듈들로 구현될 수 있다. 상기 소프트웨어 모듈들 각각은 본 명세서에서 설명되는 하나 이상의 기능 및 작동을 수행할 수 있다. 적절한 프로그램 언어로 쓰여진 소프트웨어 어플리케이션으로 소프트웨어 코드가 구현될 수 있다. 상기 소프트웨어 코드는 메모리(160)에 저장되고, 제어부(180)에 의해 실행될 수 있다.
- [0092] 한편, 전술한 단말(100)을 이용하여 여론 조사 등이 수행될 수 있다.
- [0093] 여론조사는 특정 사회 집단의 여론을 알아보는 수단으로서 여론조사 기관에서 제공하는 여론조사지를 통해 대상자들의 문항별 투표를 수집하여 결과를 도출한다.
- [0094] 여론조사의 결과는 해당 문항들에 대한 다수 여론의 성향을 나타내는 것이므로 여러 기관이나 시스템에서의 그 활용 가치가 매우 높다.
- [0095] 이로 인해 여론조사에 대한 위변조의 문제점이 고려되며 조사결과에 대한 신뢰성 보장이 중요한 이슈로 발생된다.
- [0096] 도 2는 도 1에서 설명한 단말을 기초로 제공되는 여론조사 시스템의 일례를 설명하는 블록 구성도이다.
- [0097] 도 2를 참조하면, 단말을 기초로 제공되는 여론조사 시스템(10)은 여론조사를 의뢰하는 의뢰기관(300), 사용자

의 복수의 단말(100)로부터 정보를 수집하여 여론조사와 관련된 자료를 추출하고, 의뢰기관에 제공하는 여론조사 서버(200) 등으로 구성된다.

- [0098] 여기서 의뢰기관(300), 여론조사 서버(200) 및 단말(100)은 근거리 통신 또는 원거리 통신 중 어느 하나에 따라 통신할 수 있다.
- [0099] 여기서 근거리 통신은, ANT, 블루투스(Bluetooth), RFID(Radio Frequency Identification), 적외선 통신(IrDA, infrared Data Association), UWB(Ultra Wideband), ZigBee 기술을 포함할 수 있다.
- [0100] 또한, 원거리 통신은 CDMA(code division multiple access), FDMA(frequency division multiple access), TDMA(time division multiple access), OFDMA(orthogonal frequency division multiple access), SC-FDMA(single carrier frequency division multiple access)를 포함할 수 있다.
- [0101] 한편, 도 3은 종래의 방식에 따른 여론조사 시스템의 일례를 설명하는 도면이다.
- [0102] 도 3을 참조하면, 여론조사 의뢰기관(300)으로부터 서버(200)는 의뢰를 받고, 당해 내용에 대해 협의한다.
- [0103] 이후, 서버(200)는 조사준비하고, 복수의 단말(100)로부터 자료를 수집하게 된다.
- [0104] 이때, 별도의 소프트웨어가 이용될 수도 있다.
- [0105] 이후, 서버(200)는 수집한 자료를 처리하고, 결과를 분석한 후, 의뢰기관(300)에 보고서를 제공하는 단계를 거치게 된다.
- [0106] 그러나 이러한 종래의 방식은 여론조사에 대한 위변조의 가능성이 존재하여, 조사결과에 대한 신뢰성이 보장되지 않는다는 심각한 문제점이 존재한다.
- [0107] 최근에는 위변조가 불가능한 분산 장부 관리 기법인 블록체인을 기반으로 신뢰성이 보장되는 투표 방법에 대한 연구가 등장하고 있다.
- [0108] 하지만 이와 같은 방법은 투표에 대한 기본적인 기능만을 제공하므로 다양한 문항으로 구성된 여론조사에 활용하기는 어려움이 있으며 더욱 신뢰성 있는 결과를 위한 투표결과 검증 서비스를 지원할 수 없다.
- [0109] 따라서 본 명세서에서는 이러한 문제점을 해소하고자 블록체인 기반의 여론조사 제공 방법 및 시스템을 사용자에게 제공하고자 한다.
- [0110] 구체적으로, 본 발명은 신뢰성을 보장하는 블록체인 기반의 여론조사 제공 기법 및 투표 검증 기법에 관한 것으로, 블록체인 기반의 이더리움 플랫폼 환경에서 여론조사의 생성에서부터 대상자의 관리, 투표 수행 등 기본적인 여론조사를 수행함과 동시에 개인이나 인증 기관을 통한 여론조사 결과의 검증 기능을 제안하고자 한다.
- [0111] 본 발명의 구체적인 설명에 앞서, 블록체인 및 이더리움 플랫폼에 대해 선결적으로 설명한다.
- [0112] 먼저, 블록체인(blockchain security technology)은 공공 거래 장부라고도 부르며 가상 화폐로 거래할 때 발생할 수 있는 해킹을 막는 기술이다.
- [0113] 기존 금융 회사의 경우 중앙 집중형 서버에 거래 기록을 보관하는 반면, 블록체인은 거래에 참여하는 모든 사용자에게 거래 내역을 보내 주며 거래 때마다 이를 대조해 데이터 위조를 막는 방식을 사용한다.
- [0114] 블록체인은 대표적인 온라인 가상 화폐인 비트코인에 적용되어 있는데, 비트코인은 누구나 열람할 수 있는 장부에 거래 내역을 투명하게 기록하며, 비트코인을 사용하는 여러 컴퓨터가 10분에 한 번씩 이 기록을 검증하여 해킹을 막는다.
- [0115] 다음으로, 이더리움(Ethereum)은 러시아 이민자 출신 캐나다인 비탈리크 부테린(Vitalik Buterin)이 2014년 개발한 가상화폐이다.
- [0116] 거래 명세가 담긴 블록이 사슬처럼 이어져 있는 블록체인(blockchain) 기술을 기반으로 하며 인터넷만 연결되어 있으면 어디서든 전송이 가능하다.
- [0117] 거래소에서 비트코인으로 구입하거나 비트코인처럼 컴퓨터 프로그램으로 채굴해 얻을 수 있다.
- [0118] 블록체인 기반의 분산 어플리케이션(Dapp) 제공 플랫폼인 이더리움은, 누구든지 블록체인 위에서 어떤 것이든 프로그래밍 할 수 있으며(튜링 완전성), 모든 실행 코드 및 실행 트랜잭션 내역이 공개 되어 (투명성) 분산 어플리케이션을 운영하는 것이 가능하다.

- [0119] 따라서 계약서, SNS, 이메일, 전자투표 등의 다양한 분산 어플리케이션이 존재하게 된다.
- [0120] 이하에서는, 전술한 구성 및 기술 등을 기초로 본 발명이 제안하는 블록체인 기반의 여론조사 제공 시스템에 대해 도면을 참조하여 구체적으로 설명한다.
- [0121] 도 4는 본 발명이 제안하는 블록체인 기반의 여론조사에서 여론조사 스마트 컨트랙트 구조를 설명하기 위한 도면이고, 도 5는 본 발명이 제안하는 블록체인 기반의 여론조사 시스템 개념도의 일례를 도시한 것이다.
- [0122] 본 명세서에서는 신뢰성을 보장할 수 있는 블록체인 기반의 여론조사 제공 기법과 투표 검증 기법에 대하여 제안한다.
- [0123] 제안하는 본 기법에서는 블록체인 기반의 이더리움 플랫폼 환경에서 여론조사의 생성에서부터 대상자의 관리, 투표 수행 등 기본적인 여론조사 기능을 제공하며, 또한 개인이나 인증 기관을 통한 여론조사 결과의 검증 기능을 제공한다.
- [0124] 이를 위하여 제안하는 여론조사에 필요한 이더리움 스마트 컨트랙트를 설계하고 이를 이용하여 여론조사를 수행하는 과정에 대해 도 4 및 도 5를 참조하여 설명한다.
- [0125] 본 발명에서 제안하는 기법은 블록체인 기반의 이더리움 플랫폼을 이용하여 여론조사를 수행할 수 있도록 이더리움 스마트 컨트랙트를 이용한다.
- [0126] 또한, 제안하는 투표 검증 기법은 개인이나 인증기관으로부터 여론조사 결과를 검증할 수 있는 견고한 투표 검증 기법을 제안한다.
- [0127] 여론조사 기관은 제안하는 기법을 이용하여 여론조사 정보와 여론조사의 결과를 안정적으로 관리할 수 있으며 투표 검증을 통해 신뢰성이 보장되는 여론조사 결과를 도출해 낼 수 있게 된다.
- [0128] 블록체인 플랫폼인 이더리움 환경에서의 여론조사 및 검증 기법을 제안하기 위하여 이더리움의 암호상자라 불리는 스마트 컨트랙트들의 종류와 구조를 설명한다.
- [0129] 여론조사 기관이나 대상자들은 특정 조건에서만 결과 값을 얻을 수 있는 각 스마트 컨트랙트를 이용하여 도 4와 같이 여론조사 서비스 환경을 제공받는다.
- [0130] 도 4를 참조하면, PollFactory 컨트랙트는 여론조사를 생성하고 생성된 여론조사를 관리하는 기능을 제공한다.
- [0131] PollFactory 컨트랙트를 통해 생성된 여론조사는 EthPoll라는 하나의 스마트 컨트랙트로 생성되어 그 항목 정보와 여론조사 대상자 정보를 저장한다.
- [0132] 또한, EthPoll 컨트랙트는 해당 여론조사에 대한 대상자들의 투표결과를 EthVote 컨트랙트에 저장한다.
- [0133] 여기서 EthVote 컨트랙트는 EthPoll 컨트랙트 당 하나씩 같이 생성되며 대상자들의 투표결과 보호를 위해 암호화된 상태의 투표결과를 저장한다.
- [0134] 또한, 여론조사를 제공받아 실제 투표를 진행하는 대상자들의 정보는 하나의 여론조사에 대한 대상자 관리 컨트랙트인 EthVoterStore 컨트랙트에서 관리한다.
- [0135] 또한, OrganizationStore 컨트랙트는 인증기관의 정보를 관리하며 종료된 여론조사의 전체 투표에 대한 검증 요청 시 사용된다.
- [0136] 도 5를 참조하면, 가장 먼저, 의뢰기관(300)에서 서버(200)로 조사를 의뢰하게 되고, 서버(200)는 조사를 준비한다.
- [0137] 이후, 복수의 단말(100)을 통해 사용자들로부터의 자료를 수집하게 되는데 이러한 자료는 블록체인 기반 여론조사 제공 환경에서 수집 및 분석된다.
- [0138] 이후, 자료 처리를 통해 결과가 집계되면 서버(200)는 결과를 의뢰기관(300)에 제공한다.
- [0139] 여기서 본 발명에 따르면 투표 등의 여론조사를 수행한 단말(100)의 각 사용자가 본인의 의견이 제대로 반영되었는지 여부를 확인하는 과정이 포함될 수 있다는 것이다.
- [0140] 더 나아가 여론조사 검증 기관(400)에서 별도로 서버(200)에서 진행한 자료 수집 및 분석을 수행하여 서버(200)를 통해 도출된 결과가 정확한 것인지를 확인하는 검증 과정을 진행할 수 있다.

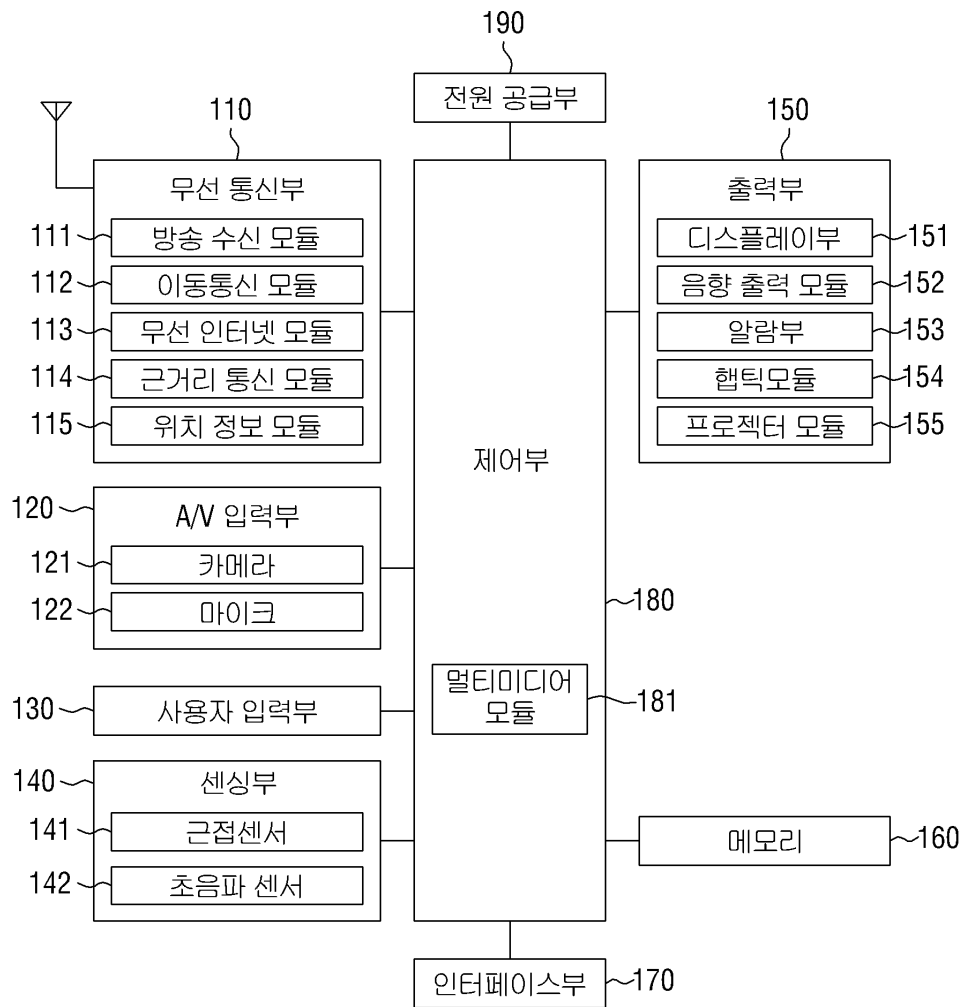
- [0141] 이는 전술한 블록체인 기반 여론조사 방식을 기초로 수행될 수 있는 것이다.
- [0142] 이하에서는 본 발명이 제안하는 시스템이 여론조사 생성, 관리 및 여론조사를 수행하는 제 1 과정과 여론조사결과를 검증하는 제 2 과정을 나누어 설명한다.
- [0143] 먼저, 도 6 및 도 7을 참조하여, 본 발명이 제안하는 시스템(10)이 여론조사 생성, 관리 및 여론조사를 수행하는 과정을 설명한다.
- [0144] 도 6은 도 5에서 설명한 블록체인 기반의 여론조사 시스템이 여론조사 생성, 관리 및 여론조사를 수행하는 과정을 설명한 것이고, 도 7은 도 6에서 설명한 여론조사 생성 과정을 보다 자세하게 설명한 액티비티 다이어그램의 일례이다.
- [0145] 도 6의 (a)를 참조하면, 여론조사 의뢰기관(300)이 서버(200) 측에 여론 조사를 의뢰하고, 도 6의 (b)와 같이 서버(200)가 제공하는 여론조사 분산 어플리케이션을 통해 단말(100)의 사용자들에 대한 명단을 준비한다.
- [0146] 이후, 도 6의 (c)와 같이, 서버(200)는 사용자들의 명단 정보를 이더리움 분산 네트워크에 분산시켜 저장하고, 도 6의 (d)와 같이, 여론 조사 대상자들에 대한 인증 작업을 수행한다.
- [0147] 이후, 도 6의 (e)에 도시된 것과 같이, 단말(100)의 사용자들이 조사 내용을 작성하고 서버(200)로 전달하면, 서버(200)는 도 6의 (f)와 같이 결과를 암호화하고, 도 6의 (g)와 같이, 이더리움 분산 네트워크로 암호화된 결과 정보를 전달한다.
- [0148] 이후, 도 6의 (h)와 (i)에 도시된 것과 같이, 결과를 서버(200)에서 복호화한 후, 해당 내용에 따라 득표 등의 처리를 함으로써, 여론 조사 결과를 도출할 수 있게 된다.
- [0149] 여론조사 기관은 여론조사의 생성에 필요한 정보를 포함하여 여론조사 서비스에 생성 요청을 보낸다.
- [0150] 생성 요청을 받은 여론조사 서비스는 서비스의 관리자에 의해 새로운 여론조사를 생성한다.
- [0151] 도 7은 여론조사 기관이 하나의 여론조사를 생성하는 과정을 나타낸 것으로, 도 7을 참조하면, 여론조사가 생성된 이후 지정된 여론조사의 시작 시각 또는 여론조사 기관의 시작 요청에 의해 여론조사가 시작된다.
- [0152] 여론조사가 시작되면 여론조사 대상자들이 여론조사 웹페이지에 접근하여 각 문항에 투표를 통해 여론조사를 작성한다.
- [0153] 작성된 여론조사의 각 투표는 대상자의 계정에 대한 개인키를 이용하여 암호화된다.
- [0154] 암호화된 원본 투표는 EthVote 컨트랙트에 저장되고 대상자의 계정정보로 복호화된 투표는 EthPoll 컨트랙트에서 해당 항목에 대한 득표로 업데이트된다.
- [0155] 다음으로, 도 8 및 도 9를 참조하여, 본 발명이 제안하는 시스템(10)이 여론조사결과를 검증하는 과정을 설명한다.
- [0156] 도 8은 도 5에서 설명한 블록체인 기반의 여론조사 시스템이 여론조사결과를 검증하는 과정을 설명한 것이고, 도 9는 도 8에서 설명한 여론조사 검증 과정을 보다 자세하게 설명한 액티비티 다이어그램의 일례를 도시한 것이다.
- [0157] 이러한 여론조사에 대한 검증 방법은 인증기관에 의한 여론조사 검증과 여론조사 대상자의 개인 투표 검증이 있다.
- [0158] 인증기관에 대한 여론조사 검증은 여론조사가 끝난 뒤 EthVote 컨트랙트의 모든 암호화된 원본 투표정보를 다시 복호화하여 검증하는 방법이며 대상자의 개인 투표 검증은 자신이 투표한 투표정보만을 복호화하는 방법이다.
- [0159] 도 8 및 도 9를 참조하면, 별도의 여론조사 검증 기관(400)이 여론조사가 끝난 뒤 EthVote 컨트랙트의 모든 암호화된 원본 투표정보를 다시 복호화하여 검증함으로써, 기존의 여론조사를 검증하는 과정이 도시된다.
- [0160] 또한, 필요에 따라 여론 조사에 응한 단말(100)의 사용자인 여론조사 대상자의 검증하는 과정도 도시된다.
- [0161] 즉, 각 단말(100)의 사용자는 득표에 사용된 데이터를 확인하거나 저장된 데이터 내용을 확인(복호화)함으로써, 기존의 여론조사의 결과를 검증할 수 있게 된다.
- [0162] 본 명세서에서는 신뢰성을 보장할 수 있는 블록체인 기반의 여론조사 제공 기법에 대하여 제안하였다.

- [0163] 본 명세서에서 제안하는 기법은 여론조사 대상자의 암호화된 투표 데이터를 블록체인에 저장하고 여론조사 검증 시에만 이를 복호화해서 재확인 가능하도록 하여 검증의 신뢰성을 높인다.
- [0164] 또한, 본 명세서에서 제안된 여론조사 기법과 견고한 투표 검증 방법은 이더리움 분산 어플리케이션에서 사용될 수 있도록 이더리움 스마트 컨트랙트로 설계되었고 그 동작 과정 또한 함께 설명하였다.
- [0165] 본 명세서에서 제안된 여론조사 제공 기법은 블록체인을 이용하여 안전하게 결과 값을 저장하면서도 매우 간단하게 결과 값을 검증할 수 있다는 점에서 여론조사에 대한 효율성과 신뢰성을 높이기 위한 해결방법으로 활용될 수 있다.
- [0166] 또한, 본 발명이 제안하는 시스템과 관련하여, 여론조사 투표데이터의 암호화 및 복호화 과정에 대해 보다 구체적으로 설명한다.
- [0167] 도 10은 본 발명이 제안하는 시스템 중 여론조사 투표데이터의 암호화 및 복호화 과정을 설명하기 위한 도면이고, 도 11a는 종래의 기존 공개키/비밀키 암호화 방법을 설명한 도면이며, 도 11b는 본 발명이 제안하는 투표데이터의 암호화 및 복호화 과정을 설명하기 위한 도면이다.
- [0168] 도 10에 도시된 시스템 구성 중 빨간 점선 박스 부분이 여론조사 투표데이터의 암호화 및 복호화 과정에 대한 내용을 나타낸 것이다.
- [0169] 종래의 암호화 과정은 대상자가 투표데이터를 암호화하고 이더리움 분산 네트워크에 전달하면, 이더리움 분산 네트워크에서는 그 암호화된 데이터를 받아 복호화하여 결과를 확인하는 방법이 적용되었으나 본 시스템에서는 보다 구체화 및 진보된 암호화 및 복호화 방법을 적용하고자 한다.
- [0170] 도 11a를 참조하면, 암호화 및 복호화 방법에는 일반적인 공개키/비밀키 쌍을 이용한 암호화/복호화 방법을 이용한다.
- [0171] 도 11a에 도시된 것과 같이, 하나의 계정(사용자)이 공개키와 비밀키를 가지고 있으며 공개키는 시스템에 공개되고 비밀키는 자신이 소지한다.
- [0172] 여기서 공개키는 비밀키와 매칭이 가능한 밀접한 관계에 있는 키로서, 이 키들은 암호화 복호화 시 다음과 같은 특징을 가진다.
- [0173] 즉, 공개키로 암호화된 데이터는 같은 쌍의 비밀키로만 풀 수 있으므로, 시스템에 알려진 특정 대상의 공개키를 이용하여 데이터를 암호화하면 해당 암호화된 데이터는 그 대상이 가진 비밀키로만 복호화를 할 수 있어 해당 대상만이 복호화하여 내용을 확인할 수 있다.
- [0174] 본 발명 건에서는 이러한 암호화 방법을 기초로 추가적인 암호화/복호화 과정이 적용된다.
- [0175] 먼저, 대상자가 암호화한 투표데이터를 복호화해서 사용하는 대상은 관리자 및 검증기관이 있는데, 관리자는 여론조사 시스템을 담당하는 대표 계정으로 대상자의 암호화된 투표데이터를 복호화하여 득표처리를 수행한다.
- [0176] 또한, 검증기관은 여론조사에 대한 검증과정을 수행하기 위해 투표데이터를 복호화한다.
- [0177] 또한, 이와 같은 두 가지 대상에 대하여 공개키/비밀키 암호화 방법을 적용하기 위해 도 11b와 같은 과정이 적용된다.
- [0178] 도 11b를 참조하면, 관리자 및 검증기관 계정은 비밀키와 공개키를 생성해서 소지하고 있다.
- [0179] 이 중 공개키는 이더리움 분산 네트워크에 배포하여 공개하게 되고, 이후, 대상자가 투표데이터를 암호화할 때 관리자와 검증기관의 공개키를 이용하여 암호화 하게 된다.
- [0180] 이렇게 각 공개키를 이용하여 암호화된 투표데이터들을 이더리움 분산 네트워크에 저장하고, 이후 관리자는 자신의 비밀키를 이용하여 자신의 공개키로 암호화된 투표데이터를 복호화하며, 그 내용에 따라 득표를 처리한다.
- [0181] 또한, 검증기관은 검증 수행 시 자신의 공개키로 암호화된 투표데이터를 자신의 비밀키로 복호화하여 내용을 검증한다.
- [0182] 이와 같은 방법을 통해 본 시스템에서는 특정 대상만이 확인할 수 있도록 암호화할 수 있게 된다.
- [0183] 한편, 상술한 본 발명의 실시예들은 다양한 수단을 통해 구현될 수 있다. 예를 들어, 본 발명의 실시예들은 하드웨어, 펌웨어(firmware), 소프트웨어 또는 그것들의 결합 등에 의해 구현될 수 있다.

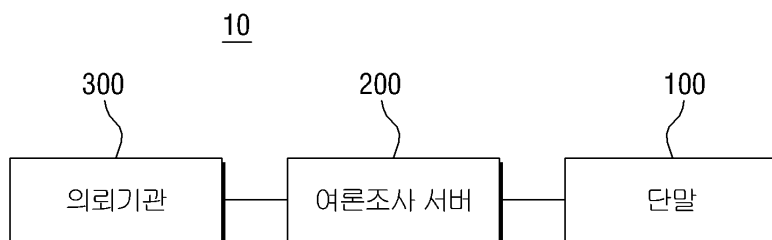
- [0184] 하드웨어에 의한 구현의 경우, 본 발명의 실시예들에 따른 방법은 하나 또는 그 이상의 ASICs(Application Specific Integrated Circuits), DSPs(Digital Signal Processors), DSPDs(Digital Signal Processing Devices), PLDs(Programmable Logic Devices), FPGAs(Field Programmable Gate Arrays), 프로세서, 컨트롤러, 마이크로 컨트롤러, 마이크로 프로세서 등에 의해 구현될 수 있다.
- [0185] 펌웨어나 소프트웨어에 의한 구현의 경우, 본 발명의 실시예들에 따른 방법은 이상에서 설명된 기능 또는 동작들을 수행하는 모듈, 절차 또는 함수 등의 형태로 구현될 수 있다. 소프트웨어 코드는 메모리 유닛에 저장되어 프로세서에 의해 구동될 수 있다. 상기 메모리 유닛은 상기 프로세서 내부 또는 외부에 위치하여, 이미 공지된 다양한 수단에 의해 상기 프로세서와 데이터를 주고 받을 수 있다.
- [0186] 상술한 바와 같이 개시된 본 발명의 바람직한 실시예들에 대한 상세한 설명은 당업자가 본 발명을 구현하고 실시할 수 있도록 제공되었다. 상기에서는 본 발명의 바람직한 실시예들을 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 본 발명의 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다. 예를 들어, 당업자는 상술한 실시예들에 기재된 각 구성을 서로 조합하는 방식으로 이용할 수 있다. 따라서, 본 발명은 여기에 나타난 실시형태들에 제한되려는 것이 아니라, 여기서 개시된 원리들 및 신규한 특징들과 일치하는 최광의 범위를 부여하려는 것이다.
- [0187] 본 발명은 본 발명의 정신 및 필수적 특징을 벗어나지 않는 범위에서 다른 특정한 형태로 구체화될 수 있다. 따라서, 상기의 상세한 설명은 모든 면에서 제한적으로 해석되어서는 아니 되고 예시적인 것으로 고려되어야 한다. 본 발명의 범위는 첨부된 청구항의 합리적 해석에 의해 결정되어야 하고, 본 발명의 등가적 범위 내에서의 모든 변경은 본 발명의 범위에 포함된다. 본 발명은 여기에 나타난 실시형태들에 제한되려는 것이 아니라, 여기서 개시된 원리들 및 신규한 특징들과 일치하는 최광의 범위를 부여하려는 것이다. 또한, 특허청구범위에서 명시적인 인용 관계가 있지 않은 청구항들을 결합하여 실시예를 구성하거나 출원 후의 보정에 의해 새로운 청구항으로 포함할 수 있다.

도면

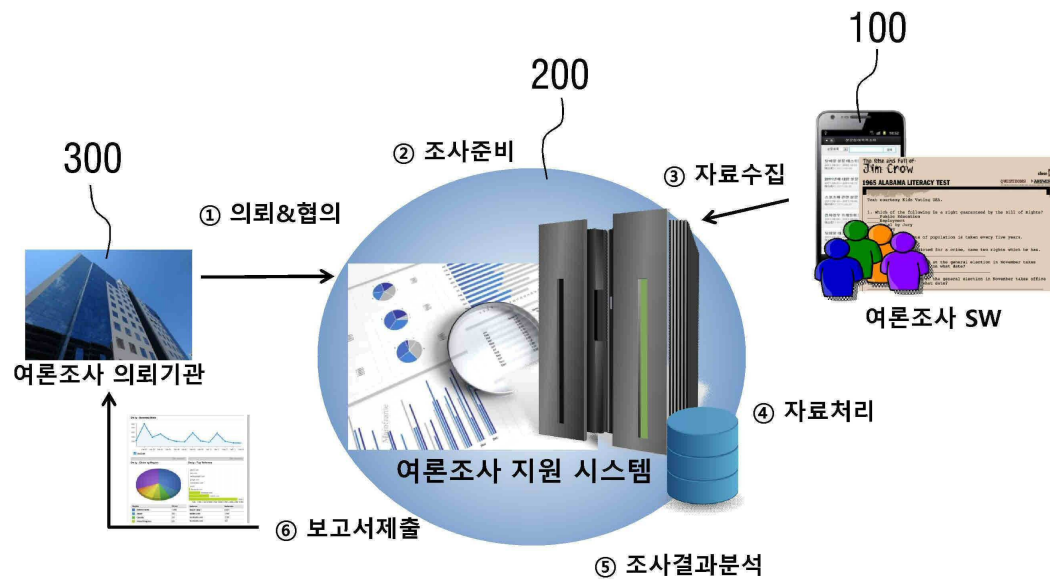
도면1



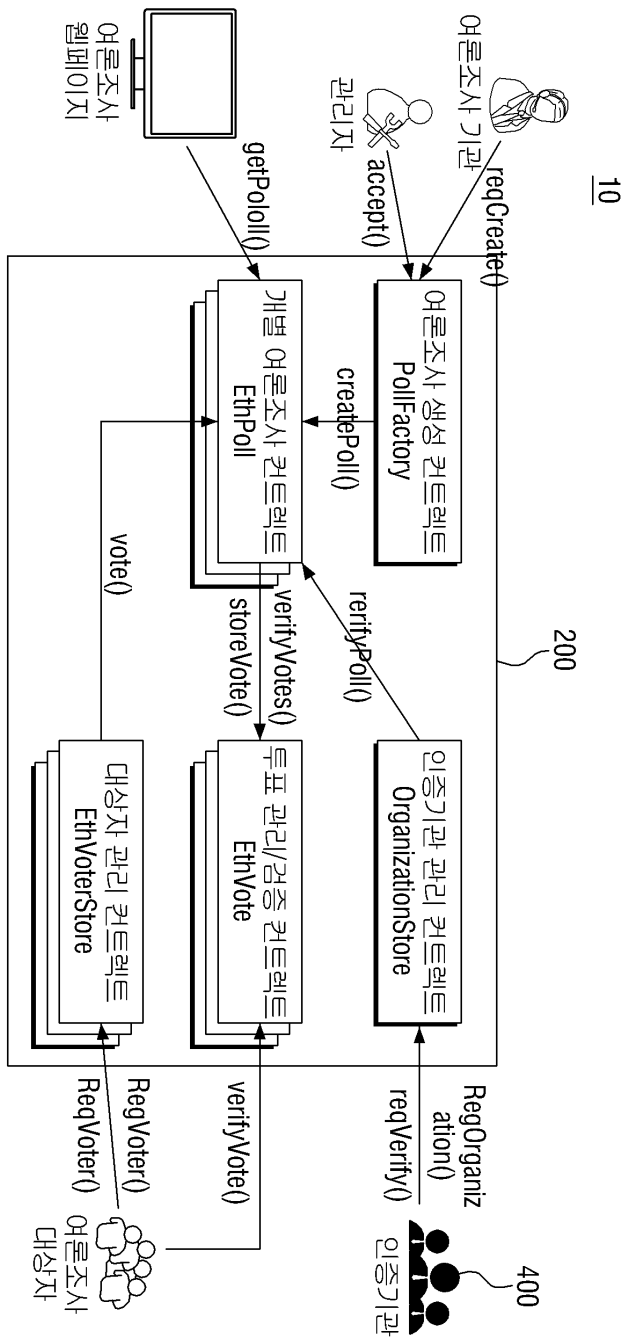
도면2



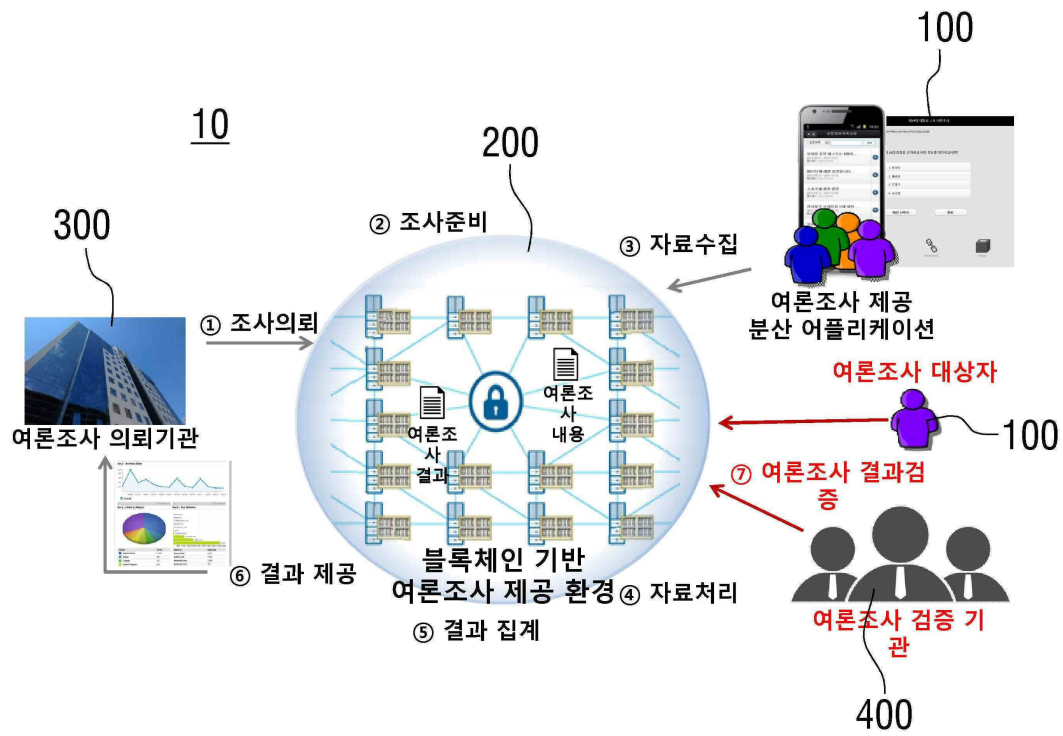
도면3



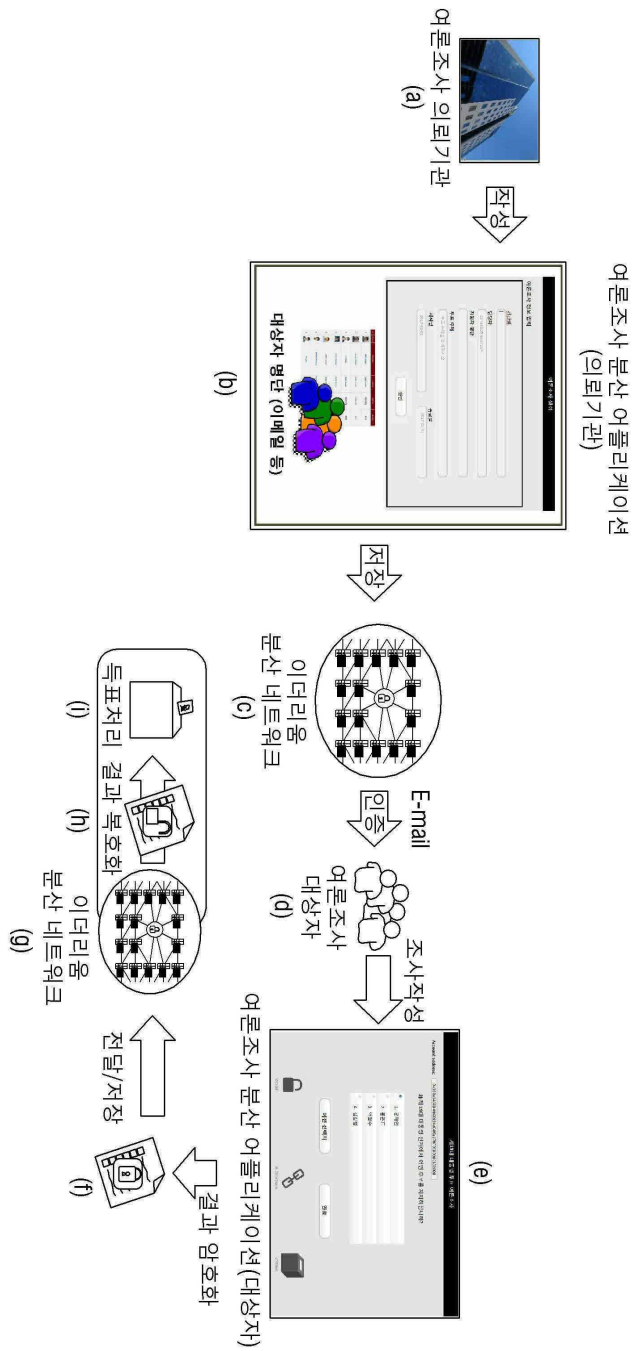
도면4



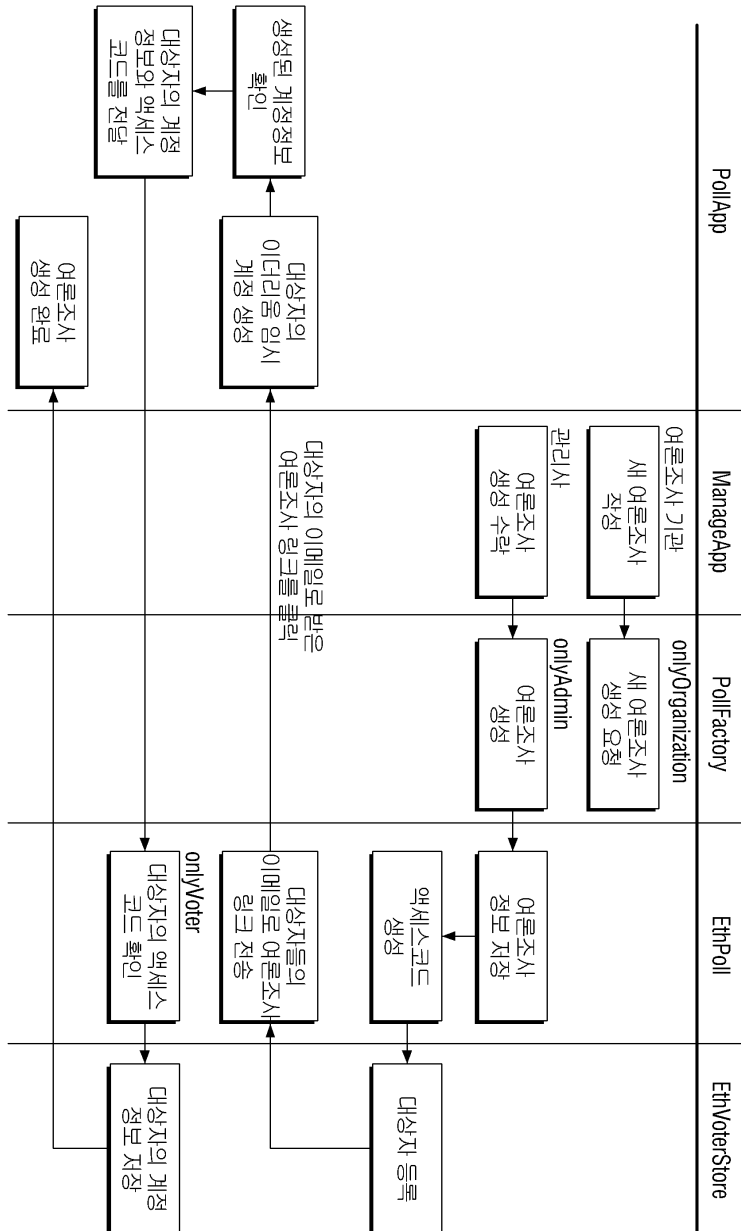
도면5



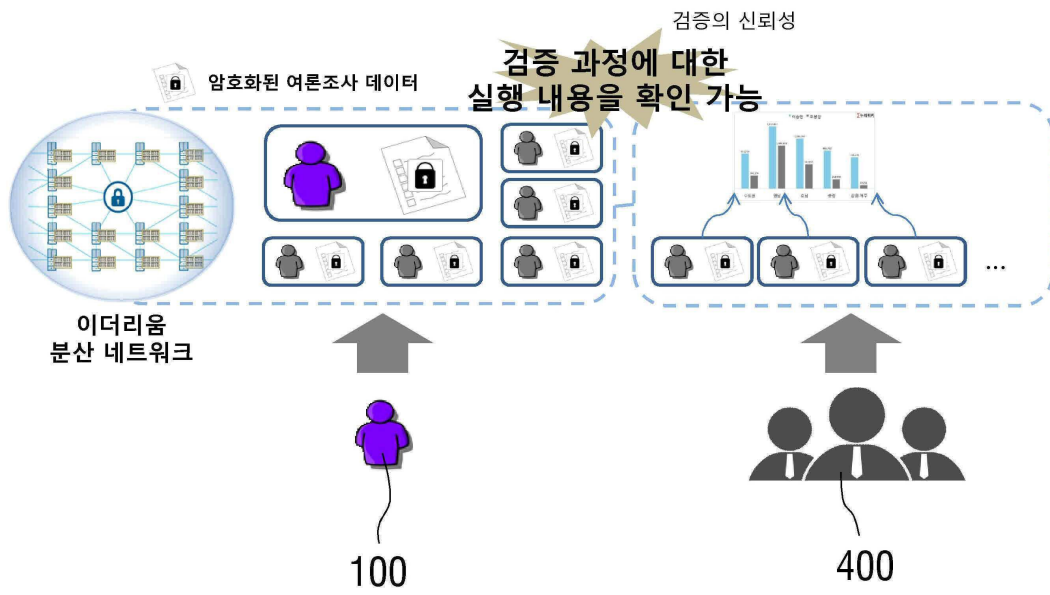
도면6



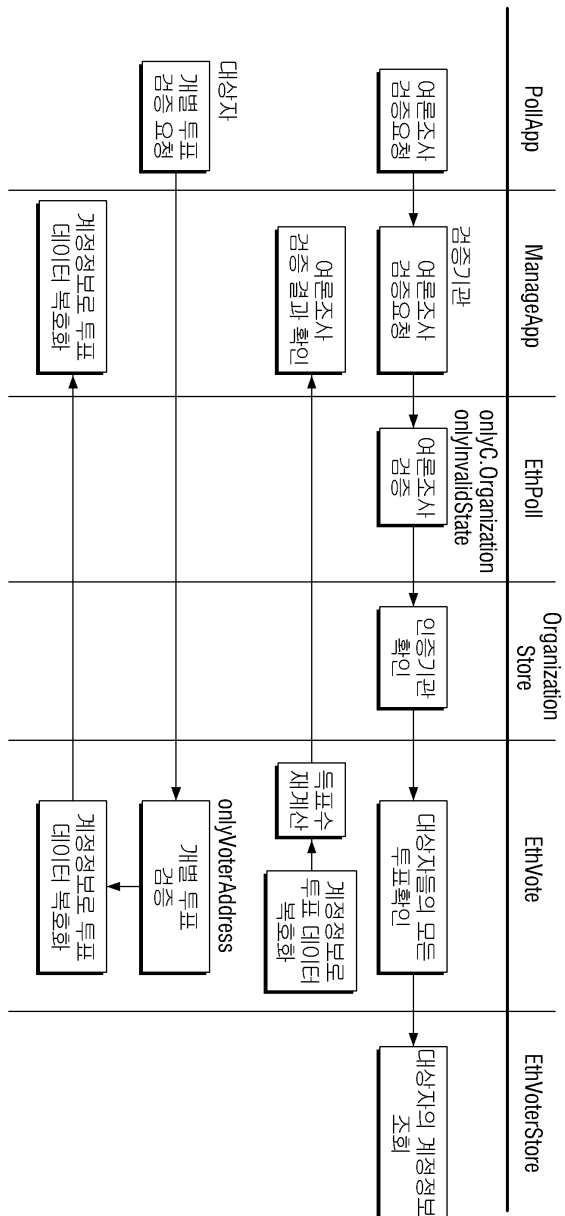
도면7



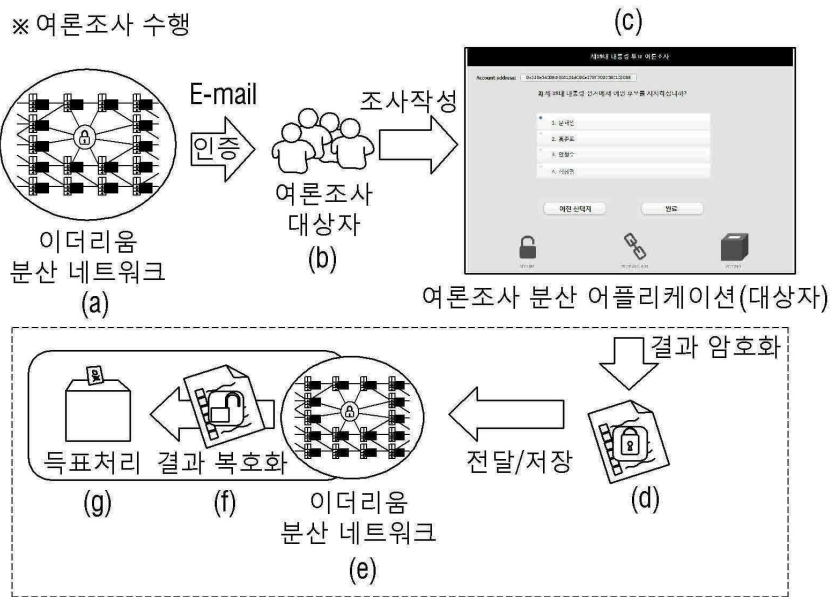
도면8



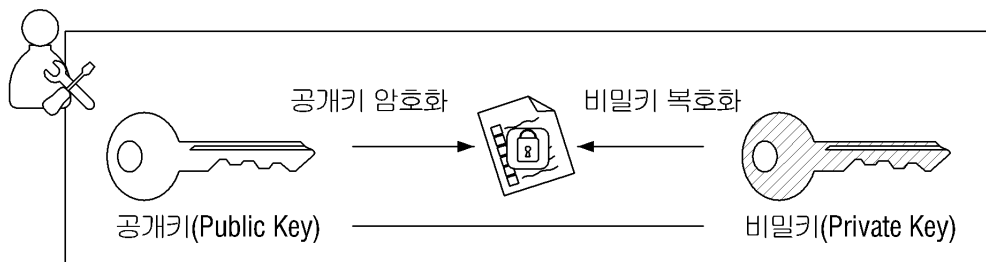
도면9



도면10



도면11a



도면11b

