(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년08월12일
(11) 등록번호 10-2288776
(24) 등록일자 2021년08월05일

(51) 국제특허분류(Int. Cl.)
*G06Q 20/06* (2012.01) *G06Q 20/38* (2012.01)
(52) CPC특허분류
*G06Q 20/065* (2013.01)
*G06Q 20/38* (2020.05)
(21) 출원번호 10-2019-0120655
(22) 출원일자 2019년09월30일
심사청구일자 2019년09월30일
(65) 공개번호 10-2020-0135119
(43) 공개일자 2020년12월02일
(30) 우선권주장
1020190061493 2019년05월24일 대한민국(KR)
(56) 선행기술조사문헌
KR1020160095720 A*
KR1020180010467 A*
KR1020180014534 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
**광주과학기술원**
광주광역시 북구 첨단과기로 123 (오룡동)
(72) 발명자
**장재혁**
광주광역시 북구 첨단과기로 123(오룡동) 광주과학기술원 전기전자컴퓨터공학부
**이홍노**
광주광역시 북구 첨단과기로 123(오룡동) 광주과학기술원 전기전자컴퓨터공학부
(74) 대리인
**김기문**

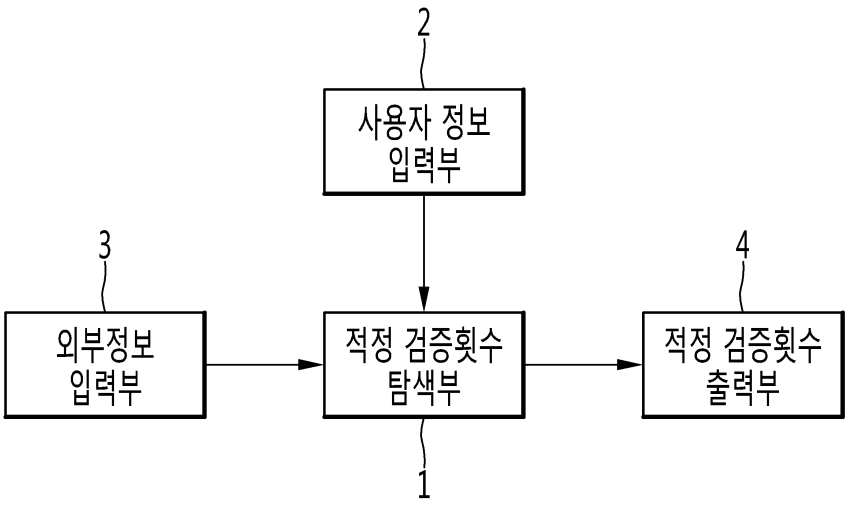
전체 청구항 수 : 총 12 항 심사관 : 이재근

(54) 발명의 명칭 **블록체인의 거래검증시스템, 및 블록체인의 거래검증방법**

## (57) 요 약

본 발명에 따른 블록체인의 거래검증시스템에는, 사용자 정보가 입력되는 사용자 정보 입력부; 암호화폐시스템과 관련되는 외부정보가 입력되는 외부정보 입력부; 상기 외부정보 및 상기 사용자 정보를 이용하여, 현재 일어나는 현재 거래의 검증에 적정한 블록검증의 수를 탐색하는 적정 검증횟수 탐색부; 및 상기 블록검증의 수를 출력하는 적정 검증횟수 출력부가 포함된다. 본 발명에 따르면, 사용자는 안전하고 신속한 거래를 위하여 필요한 블록검증의 수를 자동으로 알아낼 수 있다.

*대 표 도* - 도1



이 발명을 지원한 국가연구개발사업

| | |
|---|---|
| 과제고유번호 | 1711093581(NN24010) |
| 부처명 | 과학기술정보통신부 |
| 과제관리(전문)기관명 | 정보통신기술진흥센터 |
| 연구사업명 | 융합기술개발 |
| 연구과제명 | 확장가능한 탈중앙화 보안성 ECCPoW 블록체인 |
| 기 여 율 | 1/2 |
| 과제수행기관명 | 광주과학기술원 |
| 연구기간 | 2019.04.01 ~ 2019.12.31 |

이 발명을 지원한 국가연구개발사업

| | |
|---|---|
| 과제고유번호 | GK11380 |
| 부처명 | 광주과학기술원 |
| 과제관리(전문)기관명 | 광주과학기술원 |
| 연구사업명 | 실용화연구개발 |
| 연구과제명 | 암호-부호 작업증명(PoW) 비트코인/이더리움 하드포크 1.0개발 |
| 기 여 율 | 1/2 |
| 과제수행기관명 | 광주과학기술원 |
| 연구기간 | 2019.02.01 ~ 2019.12.31 |

공지예외적용 : 있음

# 명 세 서

## 청구범위

### 청구항 1

사용자가 입력하는 입력 거래금액이 포함된 사용자 정보가 입력되는 사용자 정보 입력부;

암호화폐시스템과 관련되는 외부정보가 입력되는 외부정보 입력부;

상기 외부정보 및 상기 사용자 정보를 이용하여, 현재 일어나는 거래의 완료를 위한 적정한 블록검증의 수를 탐색하는 적정 검증횟수 탐색부; 및

상기 블록검증의 수를 출력하는 적정 검증횟수 출력부가 포함되고,

상기 블록검증의 수(block confirmation number)는, 상기 입력 거래금액과, 상기 외부정보를 이용하여 상기 현재 일어나는 거래에서 추출되는 안전거래 한도액을 비교하여 도출되는 수인,

블록체인의 거래검증시스템.

### 청구항 2

삭제

### 청구항 3

제 1 항에 있어서,

상기 외부정보에는,

-현재 블록 하나를 채굴하면 지급되는 보상금,

-현재 블록 하나를 채굴할 때 소용되는 평균비용, 및

-현재 블록의 채굴속도,

중의 적어도 하나가 포함되는 블록체인의 거래검증시스템.

### 청구항 4

제 3 항에 있어서,

상기 외부정보에는,

-현재 블록 하나를 채굴하면 지급되는 보상금,

-현재 블록 하나를 채굴할 때 소용되는 평균비용, 및

-현재 블록의 채굴속도가,

모두 포함되는 블록체인의 거래검증시스템.

### 청구항 5

제 1 항에 있어서,

상기 적정 검증횟수 탐색부에는,

필요한 정보가 저장되는 메모리;

상기 안전거래 한도액을 추출하는 안전거래 한도액 추출부; 및

상기 안전거래 한도액과 상기 입력 거래금액을 비교하여 안전성을 판별하는 안전성 판별부가 포함되는 블록체인의 거래검증시스템.

**청구항 6**

제 5 항에 있어서,

상기 안전거래 한도액 추출부에는,

이중지불공격을 시도하는 공격자의 기대이윤을 영이 되게 만드는 금액을, 상기 안전거래 한도액으로 추출하는 연산부가 포함되는 블록체인의 거래검증시스템.

**청구항 7**

제 6 항에 있어서,

상기 공격자의 기대이윤은, 공격자의 기대수익에서 공격자의 기대비용을 감산하여 제공되는 블록체인의 거래검증시스템.

**청구항 8**

제 6 항에 있어서,

상기 안전거래 한도액($C_{Req}$)는

$C_{Req.} = (1-P_{AS})/P_{AS}*X(\gamma, t_{cut})+X(\gamma, T_{AS})-R(\beta, T_{AS})$

에 의해서 추출되고,

여기서,

$P_{AS}$(무차원)는 이중지불공격이 $t_{cut}$ 시간 내에 성공할 확률이고,

$X(\gamma,t)$는 공격자가 t 시간 동안 채굴 할 경우 소요하는 평균 블록 채굴 비용($\gamma$와 t에 대해 증가하는 함수)이고,

$\gamma$는 블록 하나를 채굴할 때 소요되는 평균비용이고,

$T_{AS}$는 공격이 성공하기까지 소요된 시간이고,

$\beta$는 블록 하나를 채굴하면 지급되는 보상금이고,

$R(\beta,t)$는 공격자가 t 시간 동안 채굴할 경우 획득하는 평균 블록 채굴 보상금($\beta$와 t에 대해 증가하는 함수)인,

블록체인의 거래검증시스템.

**청구항 9**

제 5 항에 있어서,

상기 안전거래 한도액 추출부에는 파라미터 최적화부가 포함되고,

상기 파라미터 최적화부에는,

- 공격자의 손절시간, 및

- 공격자의 자원비율 중의 적어도 하나를

최적으로 추측하는 블록체인의 거래검증시스템.

**청구항 10**

제 5 항에 있어서,

상기 안전성 판별부에 의해서 안전하지 않다고 판별되는 경우에는, 상기 블록검증의 수를 증가시켜 상기 안전거래 한도액을 다시금 추출하는 블록체인의 거래검증시스템.

**청구항 11**

암호화폐시스템에 관한 정보인 외부정보를 외부정보 입력부로 입력받고, 사용자가 입력하는 입력 거래금액이 포함된 사용자 정보를 사용자 정보 입력부로 입력받는 것;

안전하고 신속한 현재 거래의 완료를 위하여 적정한 블록검증의 수인 적정 검증횟수를 적정 검증횟수 탐색부로 탐색하는 것; 및

상기 적정 검증횟수를 적정 검증횟수 출력부로 출력하는 것이 수행되고,

상기 적정 검증횟수는, 상기 입력 거래금액과 상기 외부정보를 이용하여 상기 현재 거래에서 추출되는 안전거래 한도액을 비교하여 도출되는 수인,

블록체인의 거래검증방법.

**청구항 12**

제 11 항에 있어서,

상기 적정 검증횟수를 상기 적정 검증횟수 탐색부로 탐색하는 것은,

상기 외부정보 및 임의의 현재 블록검증의 수를 이용하여, 현재 상태에서 상기 안전거래 한도액을 안전거래 한도액 추출부로 계산하는 것;

상기 안전거래 한도액과, 상기 사용자 정보로서 입력되는 입력 거래금액을 안전성 판별부로 비교하는 것; 및

상기 안전거래 한도액과 상기 입력 거래금액을 비교하여, 상기 안전거래 한도액이 큰 경우에는 안전한 것으로 판단하고, 상기 현재 블록검증의 수를 상기 적정 검증횟수 출력부로 출력하는 것이 수행되는 블록체인의 거래검증방법.

**청구항 13**

제 12 항에 있어서,

상기 안전거래 한도액과 상기 입력 거래금액을 비교하여, 상기 안전거래 한도액이 작은 경우에는 안전하지 않은 것으로 판단하고, 상기 현재 블록검증의 수를 증가시킨 다음에, 상기 안전거래 한도액을 상기 안전거래 한도액 추출부로 다시 계산하는 것이 수행되는 블록체인의 거래검증방법.

## *발명의 설명*

### *기 술 분 야*

[0001] 본 발명은 블록체인의 거래검증시스템, 및 블록체인의 거래검증방법에 관한 것이다.

### *배 경 기 술*

[0002] 근래, 암호화폐는 상거래에서 화폐의 기능을 수행하는 단계에 이르고 있다. 상기 암호화폐를 통한 거래는 블록검증(block confirmation)을 거쳐서 거래가 완료된다. 상기 블록검증은, 거래자 간의 현재 거래행위가 일어난 이후에, 설정된 블록검증의 수에 상당하는 블록이 생성되는 것을 확인한 다음에, 거래를 완료하는 기술이다. 예를 들어, 상기 블록검증의 수가 6인 경우에는, 거래자 간의 거래가 기록되는 블록 이후에 6개의 블록이 추가로 생성되는 것을 기다린 후에 거래를 완료한다. 상기 거래완료는, 상품을 가진자가 상품을 암호화폐의 제공자에게 발송하는 것을 예시할 수 있다.

[0003] 비특허문헌 1에서는 상기 블록검증의 수가 클수록 거래가 안전하다는 것을 증명하고 있다.

[0004] 상기 블록검증은 이중지불(double spending)을 방어하는 수단으로서 활용될 수 있다. 상기 이중지불은 악의적인 사용자가, 가장 긴 블록체인이 살아남는 블록체인의 원칙을 이용하여, 실제거래의 블록체인보다 긴 악의적인 블록체인을 비밀스럽게 제공하여, 실제거래를 무산시키는 공격행위를 말한다.

[0005] 상기 블록검증의 수가 클수록 이중지불을 당할 확률은 작아진다. 그러나, 상기 블록검증의 수가 클수록 거래완

료까지 더 오랜 시간이 소요되는 문제점이 있다. 예를 들어, 비트코인(Bitcoin)의 경우에 평균 블록생성의 주기가 10분이기 때문에, 상기 블록검증의 수가 6일 경우 거래완료시간은 60분이 된다. 이 말은 콜라 한 잔을 사기 위하여 60분을 기다릴 수 있는 것이 된다. 이러한 문제점은 암호화폐의 실제사용에 큰 장애물이 되고 있다.

[0006] 이와 같은 배경 하에서, 현재 암호화폐를 이용하는 거래에서는, 거래자가 자신의 책임하에서 거래금액별로 주어지는 가이드 라인에 따라서, 블록검증의 수를 입력하도록 하는 것이 일반적이다. 거래자는, 자신의 거래에서 블록검증의 수를 얼마나 할지를 알 수가 없고, 검증횟수가 아무리 많아도 이중공격 성공확률이 영이 되지는 않는다.

## 선행기술문헌

### 비특허문헌

[0007] (비특허문헌 0001) S Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”[Online] Available: https://bitcoinorg/bitcoinpdf

## 발명의 내용

### 해결하려는 과제

[0008] 본 발명은 현재 조건에 맞추어서 적정의 블록검증의 수를 제안하는 블록체인의 거래검증시스템, 및 거래검증방법을 제안한다.

[0009] 본 발명은 거래자가 입력하는 거래금액뿐만 아니라, 다양한 외부상황에 대응하여 안전하게 신속하게 암호화폐를 통하여 거래를 완료할 수 있는, 블록체인의 거래검증시스템, 및 거래검증방법을 제안한다.

[0010] 본 발명은 암호화폐를 통한 안전한 상거래 및 신속한 거래완료의 두 목적을 함께 달성할 수 있는, 블록체인의 거래검증시스템, 및 거래검증방법을 제안한다.

### 과제의 해결 수단

[0011] 본 발명에 따른 블록체인의 거래검증시스템에는, 사용자 정보가 입력되는 사용자 정보 입력부; 암호화폐시스템과 관련되는 외부정보가 입력되는 외부정보 입력부; 상기 외부정보 및 상기 사용자 정보를 이용하여, 현재 일어나는 현재 거래의 검증에 적정한 블록검증의 수를 탐색하는 적정 검증횟수 탐색부; 및 상기 블록검증의 수를 출력하는 적정 검증횟수 출력부가 포함된다. 본 발명에 따르면, 사용자는 안전하고 신속한 거래를 위하여 필요한 블록검증의 수를 자동으로 알아낼 수 있다.

[0012] 상기 사용자 정보에는, 적어도 사용자가 입력하는 입력 거래금액이 포함되어, 사용자가 입력하는 입력거래 금액에 대응하여 안전한 거래를 신속하게 수행할 수 있다.

[0013] 상기 외부정보에는, 블록 하나를 채굴하면 지급되는 보상금, 현재 블록 하나를 채굴할 때 소용되는 평균비용, 및 현재 블록의 채굴속도 중의 적어도 하나가 포함되어, 암호화폐시스템을 이용하는 공격자의 공격경향을 파악하여 더 정확한 블록검증의 수를 알아낼 수 있다. 나아가서, 암호화폐시스템의 종류에 따라서 최적의 안전거래 한도액을 알아낼 수 있다.

[0014] 상기 외부정보에는, 블록 하나를 채굴하면 지급되는 보상금, 현재 블록 하나를 채굴할 때 소용되는 평균비용, 및 현재 블록의 채굴속도가 모두 포함되어, 보다 정확한 블록검증의 수를 알아낼 수 있다.

[0015] 상기 적정 검증횟수 탐색부에는, 필요한 정보가 저장되는 메모리; 상기 외부정보를 이용하여, 현재 상태에서 안전한 안전거래 한도액을 추출하는 안전거래 한도액 추출부; 및 상기 안전거래 한도액과 상기 입력 거래금액을 비교하여 안전성을 판별하는 안정성 판별부가 포함된다. 이에 따르면, 현재 상태를 반영하여 실시간으로 변동하는 안전한 금액을 실시간으로 알아낼 수 있다. 나아가서, 암호화폐시스템의 종류에 따라서 최적의 안전거래 한도액을 알아낼 수 있다.

[0016] 상기 안전거래 한도액 추출부에는, 공격자가 기대이윤을 영이 되게 만드는 금액을, 상기 안전거래 한도액으로 추출하는 연산부가 포함된다. 이에 따르면, 공격자의 이익에 기반하기 때문에, 공격자의 공격경향을 예측하기 때문에, 더 정확한 블록검증의 수를 알아낼 수 있다.

[0017] 여기서, 상기 공격자의 기대이윤은, 공격자의 기대수익에서 공격자의 기대비용을 감산하여 제공될 수 있다.

[0018] 여기서, 상기 안전거래 한도액($C_{Req}$)는, $C_{Req.} = (1-P_{AS})/P_{AS}*X(\gamma, t_{cut})+X(\gamma, T_{AS})-R(\beta, T_{AS})$ 에 의해서 추출될 수 있다.

[0019] 상기 안전거래 한도액 추출부에는 파라미터 최적화부가 포함되고, 상기 파라미터 최적화부에는, 공격자의 손절시간, 및 공격자의 자원비율 중의 적어도 하나를 최적으로 추측할 수 있다. 이에 다르면, 공격자의 선택 파라미터를 최적으로 예상할 수 있어서, 더 안전한 블록검증의 수를 제안할 수 있다.

[0020] 상기 안전성 판별부에 의해서 안전하지 않다고 판별되는 경우에는, 상기 블럭검증의 수를 증가시켜 상기 안전거래 한도액을 다시금 추출하도록 하는 과정이 반복될 수 있다. 이에 의해서 사용자는 가장 안전하면서 최소한 블록검증의 수를 알아낼 수 있다.

[0021] 본 발명에 따른 블록체인이 거래검증방법에는, 암호화폐시스템에 관한 정보인 외부정보 및 사용자가 입력하는 사용자 정보를 입력받는 것; 안전하고 신속한 거래를 위하여 적정한 블록검증의 수인 적정 검증횟수를 탐색하는 것; 및 상기 적정 검증횟수를 출력하는 것이 수행된다. 사용자는 안전하고 신속하게 블록체인을 통한 거래를 수행할 수 있다.

[0022] 상기 적정 검증횟수를 탐색하는 것은, 상기 외부정보 및 임의의 현재 블록검증의 수를 이용하여, 현재 상태에서 안전한 거래금액인 안전거래 한도액을 계산하는 것; 상기 안전거래 한도액과, 상기 사용자 정보로서 입력되는 입력 거래금액을 비교하는 것; 및 상기 안전거래 한도액과 상기 입력 거래금액을 비교하여, 상기 안전거래 한도액이 큰 경우에는 안전한 것으로 판단하고, 상기 현재 블록검증의 수를 출력하는 것이 수행된다. 이에 따르면, 사용자는 안전한 블록검증의 수를 알아낼 수 있거나, 실제로 블록검증의 수가 적용됨으로써, 안전하게 거래가 일어날 수 있다.

[0023] 상기 안전거래 한도액과 상기 입력 거래금액을 비교하여, 상기 안전거래 한도액이 작은 경우에는 안전하지 않은 것으로 판단하고, 상기 현재 블록검증의 수를 증가시킨 다음에, 상기 안전거래 한도액을 다시 계산하는 것이 수행된다. 이와 같은 반복계산에 의해서 실제로 가장 안전하면서 최소한의 블록검증의 수를 알아낼 수 있다.

## 발명의 효과

[0024] 본 발명에 따르면, 거래자는, 자신이 거래금액만을 입력하는 것으로써, 적정한 블록검증의 수를 알 수 있다. 여기서 적정은, 안전거래 및 신속거래의 두 목적을 합목적적으로 달성할 수 있는 것을 의미한다. 본 문서에서 적정의 의미는 위와 마찬가지로 이해할 수 있다.

[0025] 본 발명에 따르면, 현재 당사자 간의 거래만이 아니라, 당사자 간 거래의 외부에 놓이는 암호화폐전체 시스템의 상황정보(외부정보라고 할 수 있다)을 참조하여, 적정의 블록검증의 수를 제안할 수 있다. 따라서, 공격자의 선택을 예측하여 더 정확하게 상기 블록검증의 수를 제안할 수 있다.

[0026] 그 외의 상세한 구성에 따른 본 발명의 효과는 발명을 실시하기 위한 구체적인 내용에 더 상세하게 제시된다.

## 도면의 간단한 설명

[0027] 도 1은 실시예에 따른 블록체인의 거래검증시스템을 보이는 도면.

도 2는 적정 검증횟수 탐색부를 상세하게 보이는 도면.

도 3은 적정 검증횟수 탐색부의 상세한 작용을 설명하는 블록체인 거래검증방법의 일부를 설명하는 흐름도.

도 4는 안전거래 한도액 추출부의 자세한 구성을 보이는 도면.

도 5는 공격자가 점유하는 자원비율($p_A$)을 변수로 하는 안전거래 한도액의 그래프의 예시도.

도 6은 공격자가 점유하는 자원비율($p_A$)을 변수로 손절시간이 무한대일 때 공격성공을 위한 평균소요시간($\mathbb{E}_{T_{AS-ICT}}(p_A;N_{BC})$)의 그래프의 예시도.

도 7은 손절시간을 변수로 안전거래 한도액을 그래프로 예시하는 도면.

## 발명을 실시하기 위한 구체적인 내용

[0028] 이하에서는 도면을 참조하여 본 발명의 구체적인 실시예를 상세하게 설명한다. 다만, 본 발명의 사상은 이하에 제시되는 실시예에 제한되지 아니하고, 본 발명의 사상을 이해하는 당업자는 동일한 사상의 범위 내에 포함되는 다른 실시예를 구성요소의 부가, 변경, 삭제, 및 추가 등에 의해서 용이하게 제안할 수 있을 것이나, 이 또한 본 발명 사상의 범위 내에 포함된다고 할 것이다.

[0029] 도 1은 실시예에 따른 블록체인의 거래검증시스템을 보이는 도면이다.

[0030] 도 1을 참조하면, 거래검증에 필요한 검증횟수를 탐색하는 적정 검증횟수 탐색부(1), 시스템의 사용자가 입력하는 정보를 받아 상기 적정 검증횟수 탐색부(1)로 출력하는 사용자 정보 입력부(2), 암호화폐시스템의 상황정보, 즉 외부정보를 입력받아 상기 적정 검증횟수 탐색부(1)로 출력하는 외부정보 입력부(3)가 포함된다. 상기 적정 검증횟수 탐색부(1)는 적정한 블록검증의 수를 탐색하여 적정 검증횟수 출력부(4)로 출력할 수 있다.

[0031] 상기 사용자 정보 입력부(2)는 디스플레이와 입력장치를 가지는 컴퓨터 등의 입력수단이 될 수 있다. 상기 외부정보 입력부(3)는 네트워크에 연결되는 통신수단, 및 네트워크 상의 공개정보를 독출하고 저장하는 컴퓨터가 될 수 있다. 상기 적정 검증횟수 출력부(4)는 디스플레이 또는 통신수단을 가지는 컴퓨터 등의 출력수단이 될 수 있다. 상기 적정 검증횟수 탐색부(1)는 연산장치와 소정의 메모리를 가지는 컴퓨터일 수 있다.

[0032] 상기 외부정보에는, 현재 블록 하나를 채굴하면 지급되는 보상금, 현재 블록 하나를 채굴할 때 소용되는 평균비용, 및 현재 블록의 채굴속도가 포함될 수 있다.

[0033] 상기 사용자 정보에는, 사용자가 현재의 거래를 위하여 입력한 거래금액과 관련되는 정보가 포함될 수 있다.

[0034] 시스템의 사용자는 거래자라고 할 수 있다.

[0035] 실시예의 블록체인의 거래검증시스템은, 상기 사용자 정보 입력부(2)로부터 입력되는 거래금액정보, 및 상기 외부정보 입력부(3)로부터 입력되는 상기 외부정보를 이용하여, 상기 적정 검증횟수 탐색부(1)가 적정한 블록검증의 수를 탐색한다. 탐색된 정보는 적정 검증횟수 출력부(4)를 통하여 출력될 수 있다.

[0036] 사용자는, 상기 적정 검증횟수 출력부(4)에서 출력되는 블록검증의 수를 이용하여 블록검증의 수를 스스로 설정할 수 있다. 블록검증의 수에 따라서 블록검증이 수행된 다음에, 거래가 완료될 수 있다.

[0037] 사용자에 의한 상기 블록검증의 수 설정이 없이, 상기 적정 검증횟수 출력부(4)에서 출력되는 블록검증의 수가 자동으로 적용되어, 블록체인의 거래검증시스템이 운용될 수도 있다.

[0038] 도 1에 제시되는 블록체인의 거래검증시스템은 거래자의 단말기에 탑재될 수 있다.

[0039] 도 1에 제시되는 어느 단위 블럭은 거래자의 단말에, 다른 단위 블럭은 다른 거래자 및 거래소의 단말 중의 적어도 하나에 제공되어, 네트워크를 통하여 연결된 상태로, 블록체인의 거래검증시스템이 동작될 수도 있다.

[0040] 도 1에는 도시되지 않았지만, 상기 블록체인의 거래검증시스템에는, 암호화폐시스템의 임의의 다른 사용자가 블록채굴을 통하여 블록을 체인화하는 네트워크 노드가 포함되는 것은 당연히 이해할 수 있다. 즉, 네트워크 상의 적어도 하나의 다른 노드의 단말기가 협업하여, 현재의 거래를 완료하기 위하여 필요한 블록검증의 수 만큼의 블록을 체인화하여 거래검증을 완료하는 것이 당연히 포함될 수 있다.

[0041] 실시예에 따른 블록체인의 거래검증방법은, 상기 외부정보 및 상기 사용자 정보를 입력받은 다음에, 상기 적정 검증횟수를 탐색한다. 이후에는 탐색된 상기 적정 검증횟수를 출력하는 것에 의해서 수행될 수 있다

[0042] 상기 적정 검증횟수의 출력은, 사용자에게 적정 블록검증의 수가 출력된 다음에, 사용자가 블록검증의 수를 입력하는 것에 의해서 수행될 수 있다. 다른 방법으로, 자동으로 상기 적정 블록검증의 수에 따라서 자동으로 블록검증이 수행되도록 할 수도 있다.

[0043] 도 2는 상기 적정 검증횟수 탐색부를 상세하게 보이는 도면이다.

[0044] 도 2를 참조하면, 상기 적정 검증횟수 탐색부(1)에는, 현재 상태에서 안전한 수준의 검증금액을 추출하는 안전거래 한도액 추출부(10), 상기 안전거래 한도액 추출부(10)에서 추출된 안전거래 한도액과 사용자가 입력한 거래금액을 비교하여 안전성을 판별하는 안전성 판별부(12), 및 상기 안전성 판별부(12) 및 상기 안전거래 한도액 추출부(10)의 동작에 필요한 정보가 저장되는 메모리(11)가 포함될 수 있다.

[0045] 도 3은 상기 적정 검증횟수 탐색부의 상세한 작용을 설명하는 블록체인 거래검증방법의 일부를 설명하는 흐름도

이다.

[0046] 도 2 및 도 3을 참조하면, 상기 외부정보 및 상기 사용자 정보가 입력된다(S1). 상기 외부정보에는, 현재 블록 하나를 채굴하면 지급되는 보상금, 현재 블록 하나를 채굴할 때 소용되는 평균비용, 및 현재 블록의 채굴속도가 포함될 수 있다. 상기 사용자 정보에는 사용자가 입력하는 거래금액 정보가 포함될 수 있다. 상기 거래금액에는 각 나라에서 사용되는 화폐 또는 암호화폐의 액수 정보일 수 있다. 예를 들어, 원화 액수 또는 BTC 액수가 정보로서 포함될 수 있다.

[0047] 입력된 정보를 이용하여 안전거래 한도액을 계산한다(S2). 상기 안전거래 한도액은, 상기 외부정보에 의해서 예측되는, 공격자의 비용과 이익을 비교하는 것에 의해서 계산될 수 있다. 상기 안전거래 한도액의 계산은 이후에 더 상세하게 설명한다.

[0048] 상기 안전거래 한도액 계산단계(S2)에서 계산된 상기 안전거래 한도액과, 사용자 정보로서 입력된 입력 거래금액을 비교하여, 현재의 거래가 안전한 지의 여부를 판단한다(S3).

[0049] 상기 안전성 판별 단계(S3)에서, 상기 입력 거래금액과 상기 안전거래 한도액을 비교하여, 상기 입력 거래금액이 작은 경우에는 안전한 것으로 판단하여 현재 검증횟수를 출력한다(S4).

[0050] 반대로 상기 안전성 판별 단계(S3)에서, 상기 입력 거래금액이 큰 경우에는 안전하지 않은 것으로 판단하여, 검증횟수를 증가시키고(S5) 안전거래 한도액 계산단계(S2)를 다시 수행한다. 예를 들어, 현재의 검증횟수가 1인 경우에는 검증횟수를 2로 늘릴 수 있다. 이 후에는 검증횟수가 2가 되고, 현재 시점의 상기 사용자 정보 및 상기 외부정보를 이용하여, 상기 안전거래 한도액을 다시 계산할 수 있다.

[0051] 다시 수행되는 안전거래 한도액 계산단계(S2)에서는 검증횟수가 증가되었으므로, 상기 안전거래 한도액은 올라갈 것으로 예상할 수 있다.

[0052] 상기 안전거래 한도액 계산단계(S2), 및 상기 안전거래 한도액 추출부(10)의 작용은 이하에 상세하게 설명될 것이다.

[0053] 상기 안전거래 한도액은, 공격자가 이중지불공격(본 문서에서 공격이라고 하는 경우에 특별한 설명이 없는 경우에는 이중지불공격을 의미한다)을 하기 위하여 소용되는 비용과, 공격자가 이중지불공격에 성공하는 경우에 얻는 수익을 비교하는 것에 의해서 계산될 수 있다.

[0054] 예를 들어, 공격자가 공격을 하기 위하여 드는 비용에 비하여, 공격자가 공격에 성공하는 경우에 얻는 수익이 작은 경우에는, 공격자가 공격을 하지 않거나, 공격을 하더라도 성공하지 못할 것이기 때문이다.

[0055] 다시 설명하면, '공격자 기대 이윤 = 공격자의 기대 수익 - 공격자의 기대비용'에 의해서 공격자의 기대이윤이 있는 경우에는 공격자가 공격을 할 것이고, 반대로 공격자 기대이윤이 없는 경우에는 공격자가 공격을 하지 않을 것을 예상할 수 있다. 여기서, 상기 공격자 기대이윤이 영이 되는 상태의 거래금액을 상기 안전거래 한도액이라고 정의할 수 있다.

[0056] 상기 공격자의 기대수익은, 공격에 성공 할 경우의 수익(C+R)과, 공격에 실패 할 경우의 수익(영)의 합으로 주어질 수 있다. 간단하게, $P_{AS}*(C+R(\beta,T_{AS}))$로 표시할 수 있다.

[0057] 상기 공격자의 기대비용은, 공격에 성공 할 경우의 일정시간($T_{AS}$)동안 소요한 비용과, 공격에 실패 할 경우의 손절시간($t_{cut}$)시간동안 소요한 비용의 합으로 주어질 수 있다. 간단하게, $P_{AS}*X(\gamma,E[T_{AS}]) + (1-P_{AS})*X(\gamma,t_{cut})$로 주어질 수 있다. 여기서 손절시간은 손절시간이 지난 이후에는 공격에 성공할 확률이 희박하다고 판단하고 더 큰 손해를 방지하기 위해 어느 정도의 손해를 입고 공격을 그만두는 시간을 의미할 수 있다.

[0058] 결국, 상기 공격자의 기대이윤은, $P_{AS}*(C+R(\beta,E[T_{AS}])-X(\gamma,E[T_{AS}]))-(1-P_{AS})*X(\gamma,t_{cut})$로 계산될 수 있다.

[0059] 상기 안전거래 한도액$C_{Req}$)은, 공격자의 기대 이윤이 영이 되는 거래금액으로 정의할 수 있다. 따라서, 상기 공격자의 기대이윤이 영이 되도록 거래금액(C)을 좌변에 두고 우변에 나머지 항을 정리하면, $C_{Req.} = (1-P_{AS})/P_{AS}*X(\gamma,t_{cut})+X(\gamma,T_{AS})-R(\beta,T_{AS})$와 같이 정리될 수 있다.

[0060] 상기되는 설명에 제시되는 각 기호, 및 이하의 안전거래 한도액의 실제 계산에 사용되는 다양한 기호의 의미를 표 1로 정리한다.

표 1

[0061]

| 기호(단위) | 설명 | 비고 |
|---|---|---|
| C($, BTC) | 이중지불 공격대상 거래의 거래금액 | 사용자입력값 |
| β($, BTC) | 블록 하나를 채굴하면 지급되는 보상금 | 외부입력값 |
| γ($, BTC) | 블록 하나를 채굴할 때 소요되는 평균비용 | 외부입력값 |
| $\lambda_A$(No./T) | 공격자의 평균 블록채굴 속도(공격자에 따라서 다르고 알려져 있는 것 중의 최고를 이용할 수 있다)(pool에 가입해서 채굴을 하고 있고, 풀 간에 담합할 수 있다) | 외부입력값 |
| $\lambda_H$(No./T) | 일반인의 채굴속도 | 외부입력값 |
| $\lambda_T$(No./T) | 전체 채굴속도 | 외부입력값 |
| $t_{cut}$(T) | 무한정 커질 수 있는 손실을 방지하기 위한 공격제한 시간, 손절시간, cut-time | 추측검증값 |
| $p_A$(%) | 공격자가 점유한 계산 자원의 비율 | 추측검증값 |
| $N_{BC}$(No.) | 거래자가 거래를 완료하기 전 거래를 검증하는 블록검증의 수(block confirmation number) | 출력값 |
| E[$T_{AS}$](T) | 공격이 성공하기까지 소요된 평균 시간, $t_{cut}$보다 작음. | 계산값 |
| $P_{AS}$(무차원) | 이중지불공격이 $t_{cut}$ 시간 내에 성공할 확률 | 계산값 |
| R(β,t)($, BTC) | 공격자가 시간 t동안 채굴 할 경우 획득하는 평균 블록 채굴 보상금(β와 t에 대해 증가하는 함수) | 계산값 |
| X(γ,t)($, BTC) | 공격자가 시간 t동안 채굴 할 경우 소요하는 평균 블록 채굴 비용(γ와 t에 대해 증가하는 함수) | 계산값 |

[0062] 상기 비고란에는 각 기호의 값이 도출되는 방법을 나타내는 것이다.

[0063] 사용자 입력값은, 사용자가 입력하는 사용자 정보로서 여기서는 거래금액을 의미한다.

[0064] 외부입력값은, 각 암호화폐의 시스템에서 공시되고 실시간으로 변하는 값이다. 예를 들어, 상기 외부입력값은, 비트코인의 경우에는 btc.com에, 이더리움의 경우에는 etherscan.io에 공시된다.

[0065] 상기 추측검증값은, 공격자가 선택할 수 있는 값으로서 안전거래 한도액을 계산하는 중에 가장 안전한 값으로 선택될 수 있다. 상기 추측검증값은 추후에 설명될 파리미터 최적화부(16)에 의해서 최적으로 추측될 수 있다.

[0066] 상기 출력값은 본 실시예에서 일 목적으로 출력하는 값으로서, 안전한 검증횟수로서, 블록검증의 수를 나타낸다.

[0067] 상기 계산값은 상기 안전거래 한도액의 계산 중간에 사용되는 값이다.

[0068] 상기 안전거래 한도액을 계산하는 과정, 및 현재 상태에서 안전한 금액을 검출하는 안전거래 한도액 검출부(10)의 구성을 더 상세하게 설명한다.

[0069] 도 4는 상기 안전거래 한도액 추출부의 자세한 구성을 보이는 도면이다.

[0070] 도 4를 참조하면, 상기 안전거래 한도액 추출부(10)에는, 안전거래 한도액을 계산하는 연산부(15), 및 상기 연산부(15)의 연산에 필요한 파라미터를 최적화하는 파라미터 최적화부(16)가 포함된다.

[0071] 상기 파라미터 최적화부(16)는 상기 추측검증값을 최적화하는 블럭으로서, 공격자의 입장에서 공격을 예측할 수 있는 값이다.

[0072] 상기 안전거래 한도액 추출부(10)의 상세한 작용을 다수의 수학식을 참조하여 상세하게 설명한다. 이하의 설명에 있어서 상기 파라미터 최적화부(16)의 작용에 대한 언급이 없는 부분은 모두 상기 연산부(15)에서 수행하는 것으로 이해할 수 있다.

[0073] 하기 수학식 1은 채굴비용/시간의 단위를 채굴비용/블록의 단위로 변환하는 것을 예시한다.

*수학식 1*

$$\gamma = 4.63 \cdot 10^{-22}\ [\mathrm{BTC/hash}] \times 456\mathrm{E}[\mathrm{hashes/block\ mining}] \approx 0.21\ [\mathrm{BTC/block\ mining}].$$

[0074]

[0075] 상기 수학식 1을 참조하면, 상기 외부정보로서 알려져 있는 채굴비용/해쉬와 해쉬수/블록을 곱하는 것으로서, 블록당 채굴비용을 얻어낼 수 있다. 수학식 1의 결과는 메모리에 저장될 수 있다.

[0076] 하기 수학식 2는 공격자의 채굴속도를 알아내는 것을 예시한다.

*수학식 2*

$$p_A := \Pr(S_i = n+1 \mid S_{i-1} = n) = \frac{\lambda_A}{\lambda_T},$$

$$p_H := \Pr(S_i = n-1 \mid S_{i-1} = n) = \frac{\lambda_H}{\lambda_T},$$

[0077]

[0078] 상기 수학식 2에서 람다는 속도이고, H(honest)는 일반인이고, T(Total)는 전체를 의미하고, A(Attacker)는 공격자를 의미하고, $p_A$는 공격자가 가지는 자원의 비율이고, $p_H$는 일반인이 가지는 자원의 비율이다. $p_H$에서 소문자 p는 proportion의 두문자로 이해할 수 있다.

[0079] 상기 수학식 2를 통하여 공격자의 채굴속도($\lambda_T$)를 알아낼 수 있다. 상기 수학식 2의 결과는 상기 메모리(11)에 저장될 수 있다. 상기 메모리(11)에는 상기 채굴비용 및 상기 채굴속도뿐만 아니라, 연산에 필요한 정보가 필요에 따라서 저장될 수 있다.

[0080] 하기 수학식 3은 손절시간이 무한대로 공격할 경우에 공격에 성공할 확률로서, 비특허문헌에 인용되는 사토시 나카모토의 논문에 의해서 공지되어 있다.

*수학식 3*

$$\mathbb{P}_{AS-ICT}(p_A; N_{BC}) = \begin{cases} 1, & p_H \le p_A, \\ 1 - p_A^{N_{BC}+1} p_H^{N_{BC}} \sum_{j=N_{BC}}^{2N_{BC}} \binom{j-1}{N_{BC}-1} A_j, & p_H > p_A, \end{cases}$$

*where*

$$A_j \triangleq p_A^{j-2N_{BC}-1} - p_H^{j-2N_{BC}-1}.$$

[0081]

[0082] 상기 수학식 3에서 P는 확률(probality)를 의미하고, AS(attack success)는 공격성공을 의미하고,

ICT(infinite cut time)으로서 손절시간이 무한한 것을 의미하고, $N_{BC}$는 검증을 위한 블록검증의 수를 의미한다.

[0083] 하기 수학식 4는 상기 수학식 3에 의해서 도출되는 식으로서, 주어진 시간 내에 공격에 성공할 확률에 관한 확률분포를 나타낸다.

*수학식 4*

[0084]
$$f_{T^{(1),(2)}}(t)=\frac{p_A\lambda_T e^{-\lambda_T t}\left(p_A p_H(\lambda_T t)^2\right)^{N_{BC}}}{(2N_{BC})!}\cdot\sum_{j=N_{BC}}^{j=2N_{BC}}\binom{j-1}{N_{BC}-1}\,{}_2F_3\left(\mathbf{a};\mathbf{b};p_A p_H(\lambda_T t)^2\right)+\frac{e^{-\lambda_T t}}{t}\frac{(p_H\lambda_T t)^{N_{BC}}}{(N_{BC}-1)!}\left(e^{p_A\lambda_T t}-\sum_{i=0}^{N_{BC}}\frac{(p_A\lambda_T t)^i}{i!}\right)+(1-\mathbb{P}_{AS-ICT})\delta(t-\infty),$$

[0085] 상기 수학식 4는 여기서 ${}_pF_q$는 [G Gasper and M Rahman, “Basic Hypergeometric series,” in *Basic hypergeometric series*, Second, vol 96, Cambridge University Press, Cambridge, 2004]에 정의되는 일반화 초기하학적 함수(generalized hypergeometric function)이고, a, b는 수학식 5에 정의된다.

*수학식 5*

[0086]
$$\mathbf{a}=\begin{bmatrix}N_{BC}+1-j/2\\ N_{BC}+1/2-j/2\end{bmatrix}$$

$$\mathbf{b}=\begin{bmatrix}2N_{BC}+2-j\\ N_{BC}+1\\ N_{BC}+1/2\end{bmatrix}.$$

[0087] 상기 수학식 4의 확률분포를 제 1 적분하여, 하기 수학식 6의 손절시간 내에 공격에 성공할 확률을 알아낼 수 있다.

*수학식 6*

[0088]
$$\mathbb{P}_{AS}(p_A,t_{cut};N_{BC}):=\Pr\left(T^{(1),(2)}<t_{cut}\right)$$

[0089] 상기 수학식 5의 확률분포를 제 2 적분하여, 하기 수학식 7의 손절시간 내에 공격에 성공하는데 소요되는 평균 시간을 알아낼 수 있다.

*수학식 7*

$$\mathbb{E}_{T_{AS}}\left(p_A, t_{cut}; N_{BC}\right) = \frac{\int_0^{t_{cut}} t f_{T^{(1),(2)}}(t)\,dt}{\mathbb{P}_{AS}\left(p_A, t_{cut}; N_{BC}\right)}$$

[0090]

[0091] 여기서, E(expectation)은 기대값이고, P(probality)는 확률이고, f는 확률론에서의 확률분포이다.

[0092] 상기 수학식 6과 수학식 7을 이용하여, 공격자의 평균공격비용을 수학식 8과 같이 알아낼 수 있다.

*수학식 8*

$$\begin{aligned}\mathbb{E}_X\left(p_A, t_{cut}; N_{BC}\right) :=\\ \mathbb{P}_{AS}\left(p_A, t_{cut}; N_{BC}\right)\mathbb{E}\left[X\left(\lambda_A, T_{AS}\right)\right]\\ +\left(1-\mathbb{P}_{AS}\left(p_A, t_{cut}; N_{BC}\right)\right)X\left(\lambda_A, t_{cut}\right)\end{aligned}$$

[0093]

[0094] 여기서, X는 채굴비용을 나타낸다. 상기 채굴비용 X를 선형함수로 제공하는 것은, 채굴장비를 인터넷 상의 대여소(예를 들어, nicehach.com)를 통하여 대여하는 비용을 선형함수로 예시한 것이다. 만약, 상기 채굴비용이 대여비용이 아닌 장비의 전기사용료 등이 되는 경우와 같이 다양한 경우에 대응하여, 상기 비용함수 X는, n-제곱함수, n-루트함수, 로그함수, 지수함수, 또는 n-루트 함수가 될 수도 있을 것이다.

[0095] 한편, 수학식 3을 이용하여, 손절시간이 무한대일 때 공격성공을 위한 평균소요시간($\mathbb{E}_{T_{AS-ICT}}\left(p_A; N_{BC}\right)$)을 수학식 9와 같이 알아낼 수 있다.

*수학식 9*

$$\mathbb{E}_{T_{AS-ICT}}\left(p_A; N_{BC}\right) = \frac{\lambda_T^{-1}\left(\sum_{j=N_{BC}}^{2N_{BC}} \binom{j-1}{N_{BC}-1} Z_j + \frac{N_{BC}}{p_H}\right)}{\mathbb{P}_{AS-ICT}\left(p_A; N_{BC}\right)};$$

*where*

$$Z_j := p_A p_m^{N_{BC}} p_M^{-(N_{BC}-j+1)}\left(\frac{2N_{BC}-2jp_m+1}{p_M-p_m}\right) - jp_A^{-(N_{BC}-j)} p_H^{N_{BC}}.$$

[0096]

[0097] 상기 수학식 9를 이용하여, 공격자가 점유하는 자원을 예측하여 가장 안정된 검증금액을 제시하는, 공격자가 점유하는 자원비율($p_A$)을 알아낼 수 있다.

[0098] 구체적으로, 상기 수학식 9를 참조하면, 손절시간이 무한대일 때 공격성공을 위한 평균소요시간($\mathbb{E}_{T_{AS-ICT}}\left(p_A; N_{BC}\right)$)은, 공격자가 점유하는 자원비율($p_A$)을 인자로 하는 함수이다. 이 경우에, 공격자가 점유

하는 자원비율($p_A$)을 변수로 손절시간이 무한대일 때 공격성공을 위한 평균소요시간($\mathbb{E}_{T_{AS-ICT}}(p_A;N_{BC})$)을 계산하면, 도 6과 같이 아래로 볼록한 함수로 나타난다.

[0099] 따라서, 도 6의 그래프 상에서, 가장 낮은 곳의 공격자가 점유하는 자원비율($p_A$)을 취하여, 공격자가 점유하는 자원비율을 가장 안정적으로 최적화할 수 있다. 공격자는 가장 최소의 비용으로 빠른 공격 효과를 얻어낼 수 있는 점유 자원비율을 선택할 것이기 때문이다.

[0100] 이때 상기 공격자가 점유하는 자원비율에 대한 최적화는 상기 파라미터 최적화부(16)에 의해서 연산부(15)와는 별개의 작용을 통하여 수행될 수 있다. 상기 차라미터 최적화부(16)에서 최적화된, 상기 공격자가 점유하는 자원비율은 상기 연산부(15)로 피드백되어 상기 안전거래 한도액의 획득에 사용될 수 있다.

[0101] 이후에는 상기 안전거래 한도액을 얻기 위하여 하기 수학식 10이 적용된다.

*수학식 10*

[0102]
$$C_{\text{Req.}}=\frac{\mathbb{E}_X(p_A,t_{cut};N_{BC})}{\mathbb{P}_{AS}(p_A,t_{cut};N_{BC})}-\mathbb{E}\left[R(\lambda_A,T_{AS})\right]$$

[0103] 상기 수학식 10에서 R은 보상금으로서 R은 하기 수학식 11과 같이 주어질 수 있다.

*수학식 11*

[0104]
$$R(\lambda_A,t):=\beta\lambda_A t\left(\log_{r_1} r_2\right)^{\lambda_A}\left(\log_{r_3} r_4\right)^{t}$$

[0105] 상기 수학식 11에서 로그텀(log term)은, 보상금이 시간에 대하여 로그함수 또는 지수함수로 가능한 것으로 보이는 것이다. 다만, 시간에 비례하는 함수로 주어지는 경우에는 로그텀들은 모두 1로 주어질 수 있다.

[0106] 다만, 상기 보상금 R도, 채굴비용(X)과 마찬가지로, n-제곱함수, n-루트함수, 로그함수, 지수함수, 또는 n-루트 함수가 될 수도 있을 것이다.

[0107] 다시 수학식 10을 참조하면, 여전히 손절시간($t_{cut}$)은 알려지지 않았고, 수학식 10은 손절시간을 인자로 하는 함수로 주어질 수 있다. 따라서, 손절시간을 변수로 하여 안전거래 한도액($C_{req}$)를 최적화할 수 있다.

[0108] 상기 손절시간을 변수로 상기 안전거래 한도액을 그래프로 예시하는 도면이 도 7에 도시된다.

[0109] 도 7을 참조하면, 상기 손절시간에 대하여 상기 안전거래 한도액은 아래로 볼록한 그래프로 나타난다. 가장 안전거래 한도액으로서 가장 낮은 검증금액을 출력할 수 있다. 상기 손절시간에 대응하여 상기 안전거래 한도액의 최적값을 구하는 작용은 상기 파라미터 최적화부(16)를 통하여 수행될 수 있다.

[0110] 상기 파라미터 최적화부(16)는, 현재 상태에서 가장 낮은 상기 안전거래 한도액을, 상기 연산부(15)로 출력할 수 있다.

[0111] 한편, 이상의 설명은 공격자의 자원비율이 50이하인 경우에 적용될 수 있다.

[0112] 반대로 공격자의 자원비율이 50%를 초과하는 경우에는 이미 설명한 바와 같이, 공격자는 손절시간을 무한대로 설정할 수 있다. 왜냐하면, 자원이 50%를 초과하는 경우에는 언젠가는 자원이 우세하므로 공격자가 언젠가는 더 긴 블록체인을 만들 수 있기 때문이다.

[0113] 상기 공격자의 자원비율이 50%이하인 경우(이하 50%공격이라고 한다)와, 상기 공격자의 자원비율이 50%초과하는 경우(이하에서는 51%공격이라고 한다)에, 추측검증값인, 공격자의 손절시간($T_{cut}$) 및 공격자의 자원비율($P_A$)의 최

적화에 대하여 상세하게 설명한다.

[0114] 상기 공격자의 손절시간($T_{cut}$) 및 공격자의 자원비율($P_A$)의 최적화는 상기 파라미터 최적화부(16)에서 수행될 수 있다.

[0115] 일반적으로, 51% 공격의 최적 검증횟수가 50% 공격의 최적 검증횟수보다 더 크다. 비트코인과 같은 계산자원의 규모가 거대한 네트워크에서는 특정 집단이 51% 이상의 계산 자원을 확보하기가 매우 어렵다. 따라서 50% 공격에 대한 대비를 하는 것으로도 충분하다. 반대로 계산자원의 규모가 작은 네트워크에서는 51% 공격이 가능할 수 있기 때문에 더욱 철저한 대비가 필요하다.

[0116] 첫번째로, 상기 51% 공격의 상황에서, 공격자에게 최선의 손절시간은 무한대이고, 최적의 공격자원 점유율은 계산가능하다.

[0117] 손절시간이 유한한 경우와 무한한 경우에 대해 이윤을 비교할 수 있다. 예를 들어, 블록 하나를 채굴할 때의 보상금(β)이 블록 하나를 채굴할 때의 비용(γ)보다 큰 경우, 즉 채굴로 얻는 시간당 보상이 채굴로 소요하는 시간당 비용보다 큰 경우에서는, 손절시간이 무한한 경우의 공격 이윤이 가장 크다.

[0118] 반대로, 블록 하나를 채굴할 때의 보상금(β)이 블록 하나를 채굴할 때의 비용(γ)보다 작은 경우에는 손절시간이 무한한 경우의 공격 이윤이 항상 가장 크다고 할 수는 없지만, 대부분의 실질적인 경우에서는 그러하다. 뿐만 아니라 정상적인 네트워크는 시장경제에 의해 β가 γ보다 크도록 형성되어있는 것이 보통이다.

[0119] 51% 공격 상황에서 손절시간이 무한할 때, 상기 안전거래 한도액($C_{Req.}$)은 공격자가 가지는 자원비율($p_A$)에 대해 아래로 볼록인 함수이며, 이는 수학적으로 증명된 바가 있고 도 5와 같이 실제로 예시된다.

[0120] 즉, 공격자가 가지는 자원비율($p_A$)에 대해 상기 안전거래 한도액($C_{Req}$)의 하한이 존재한다. 상기 입력 거래금액(C)과 상기 안전한 검증금액($C_{Req}$)을 비교하여 $C<C^{*}_{Req.}$를 만족하면, 공격자가 가지는 모든 자원비율에 대해 $C<C_{Req.}$이므로, 거래가 안전함을 알 수 있다. 따라서, 거래자는 안전성을 판단하기 위하여, 공격 자원 점유율이 최악의 경우만 고려하면 된다. 예를 들어, 도 5에서 가장 가장 낮은 상기 안전거래 한도액을 선택하면 된다.

[0121] 두 번째로 50% 공격 상황에서도 공격자에게 최적의 손절시간($t_{cut}$)과 가장 합리적인 공격자가 가지는 자원비율($p_A$)를 고려해 볼 수 있다.

[0122] 상기 50% 공격의 경우에는 공격성공 평균시간이 최소화되는 공격자가 가지는 자원비율($p_A$)이 합리적인 공격 자원 점유율이다. 50% 공격인 경우에는 51% 공격과는 다르게 무한한 손절시간을 고려 할 필요가 없는데, 이는 공격자의 기대 손실이 무한히 커지기 때문이다.

[0123] 따라서 공격자는 반드시 유한한 손절시간의 선택이 강제된다. 공격자의 입장에서는 손절시간을 선택할 때 공격이 성공하기까지 소요되는 평균 시간, 즉 공격성공 평균시간을 고려하지 않을 수 없다. 예를 들어 공격성공 평균시간이 알려져 있다면, 공격을 시도 할 때 손절시간을 공격성공 평균시간, 그보다 조금 더 큰 시간, 혹은 그보다 수 배 큰 시간으로 설정 할 수 있다.

[0124] 50% 공격의 경우에는 공격 성공확률이 그리 높지 않으므로, 공격자는 공격을 여러 회 시도하여 이윤을 취할 것이다. 그러므로 매 회의 공격 시도에 걸리는 시간이 길면 길수록 적자에서 흑자로 전환되는데 걸리는 시간이 늦어질 것이다. 신속하고 정확하게 손절시간을 찾기 위해, 공격자는 공격성공 평균시간이 최소화 되는 공격자가 가지는 자원비율($p_A$)을 탐색할 것이다.

[0125] 공격성공 평균시간이 도 6과 같이 아래로 볼록인 함수, 즉 최소값이 존재하는 함수임을 계산적으로 확인하였다. 따라서 50% 공격의 경우에는 공격성공 평균 간이 최소화되는 공격자가 가지는 자원비율($p_A$)를 합리적인 공격 자원 점유율로 가정할 수 있다.

[0126] 또한, 50% 공격에서 공격자가 가지는 자원비율($p_A$)이 고정되어 있을 때, 상기 안전거래 한도액($C_{Req}$)은 $t_{cut}$에 대해 아래로 볼록인 함수임을 도 7과 같이 확인 하였다. 즉, 손절시간에 대하여 상기 안전거래 한도액의 하한이 존재한다. 따라서 거래자는 안전성을 판단하기 위해 손절시간이 최악의 경우, 즉 상기 안전거래 한도액이 가장 낮은 경우만 고려하면 된다.

[0127] 공격자의 자원비율이 50%를 초과하는 경우에는 이미 설명한 바와 같이, 공격자는 손절시간을 무한대로 설정할

수 있다.

[0128] 이 경우에는 수학식 9에 제시되는, 손절시간이 무한대일 때 공격성공을 위한 평균소요시간 ($\mathbb{E}_{T_{AS-ICT}}(p_A;N_{BC})$)을 이용하여, 하기 수학식 12와 같이 상기 안전거래 한도액을 알아낼 수 있다. 다시 말하지만, 이 경우에 손절시간은 무한대이다.

*수학식 12*

[0129] $$C_{\text{Req.}} = \max\left(0,(\gamma-\beta)\lambda_T p_A \mathbb{E}_{T_{AS-ICT}}(p_A;N_{BC})\right)$$

[0130] 상기 수학식 12를 참조하면, 공격자가 점유하는 자원비율($p_A$)은 알려지지 않았고, 수학식 12는 공격자가 점유하는 자원비율($p_A$)을 인자로 하는 함수로 주어질 수 있다. 따라서, 공격자가 점유하는 자원비율($p_A$)을 변수로 하여 안전거래 한도액($C_{req}$)를 최적화할 수 있다. 상기 최적화는 상기 파라미터 최적화부(16)에서 수행될 수 있다.

[0131] 공격자가 점유하는 자원비율($p_A$)을 변수로, 상기 안전거래 한도액을 그래프로 예시하는 도면이 도 5로 이미 설명된 바가 있다.

[0132] 도 5를 참조하면, 상기 공격자가 점유하는 자원비율($p_A$)에 대하여 상기 안전거래 한도액은 아래로 볼록한 그래프로 나타난다. 가장 안전거래 한도액으로서 가장 낮은 검증금액을 출력할 수 있다.

[0133] 본 문서에 기재되는 기술에 다르면, 사용자가 거래금액만을 입력하는 것에 의해서 적정 검증횟수를 출력하고, 상기 적정 검증횟수에 따라서 블록검증의 수를 설정할 수 있다. 이에 따르면, 안전하고 신속한 암호화폐를 이용한 상거래가 가능한 장점이 있다.

[0134] 또한, 거래의 안정성을 판단하기 위한 기준으로서, 상기 안전거래 한도액을 계산하는 과정에 추측되어야 하는 추측검증값이 최적화됨으로써, 사용자가 거래금액만을 입력하더라도 적정한 블록검증의 수를 알아낼 수 있다.

## *산업상 이용가능성*

[0135] 본 발명에 따르면, 암호화폐를 통한 상거래를 안전하고 신속하게 수행할 수 있도록 함으로써, 암호화폐를 이용하는 실물거래를 더욱 촉진할 수 있다.

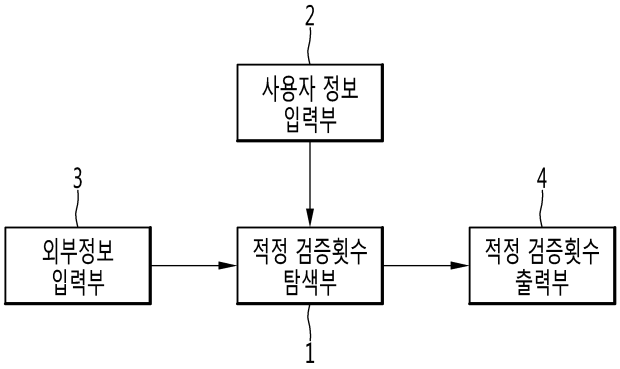
## *부호의 설명*

[0136] 10: 안전거래 한도액 추출부

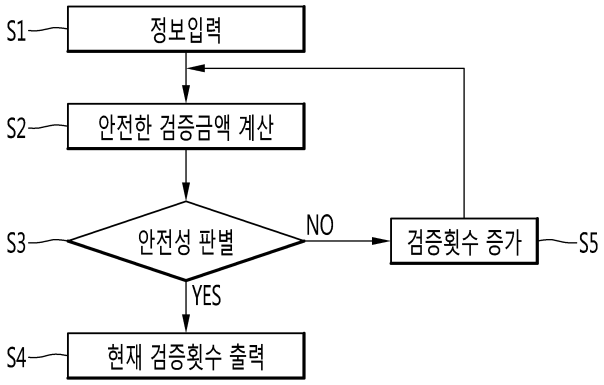
12: 안전성 판별부

## 도면

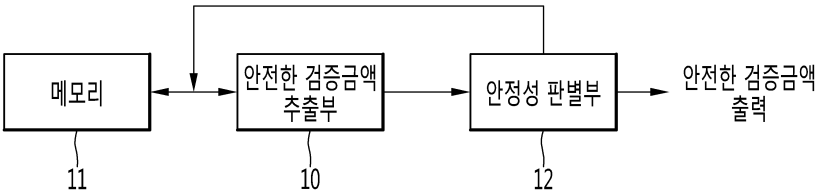
### 도면1



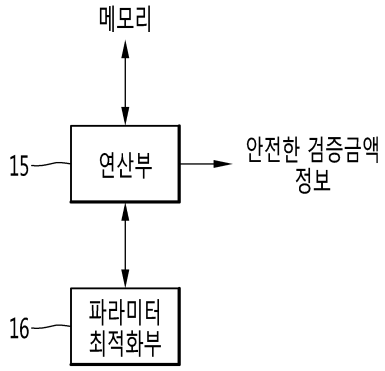

### 도면2



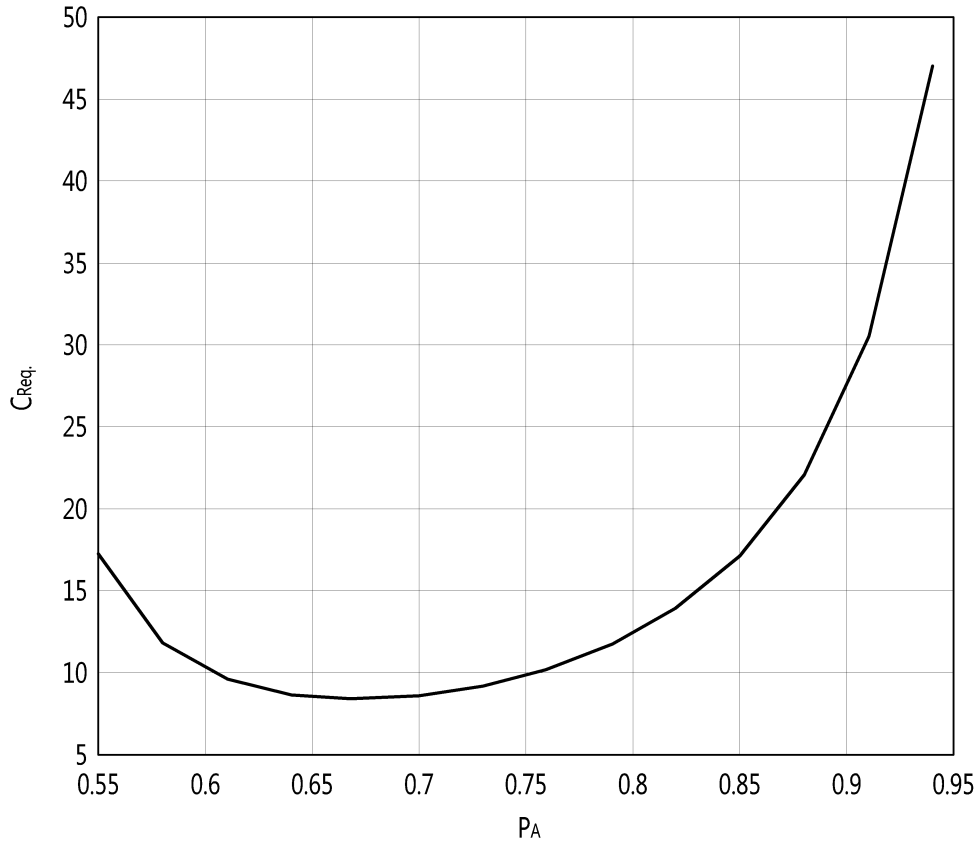

### 도면3



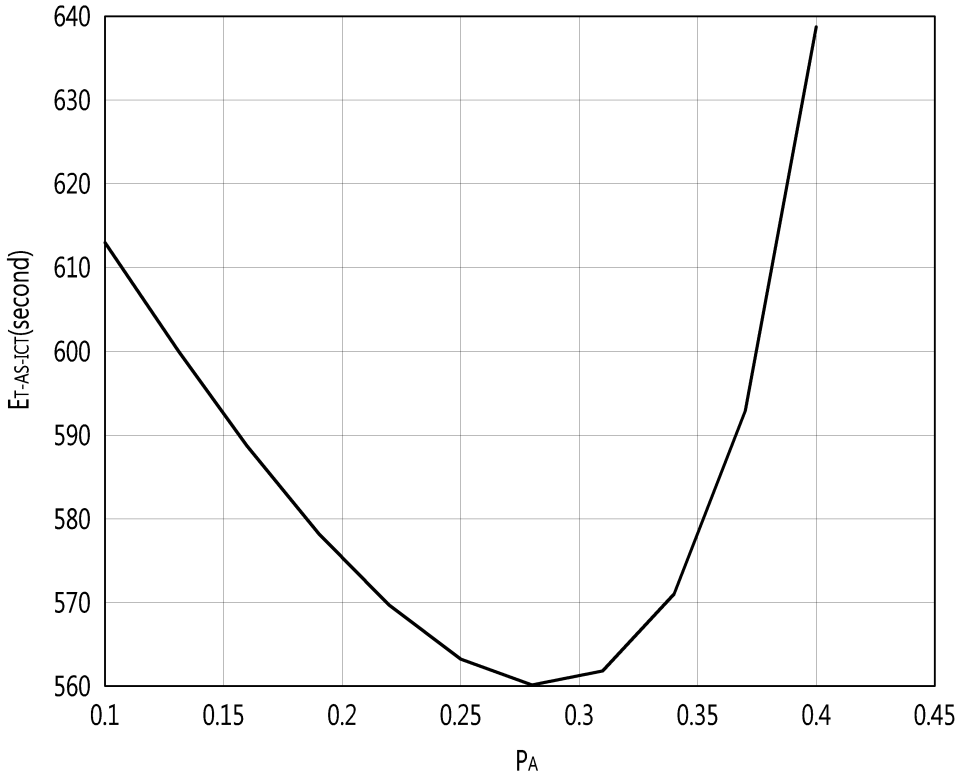
도면4


메모리
15
연산부
안전한 검증금액
정보
16
파라미터
최적화부

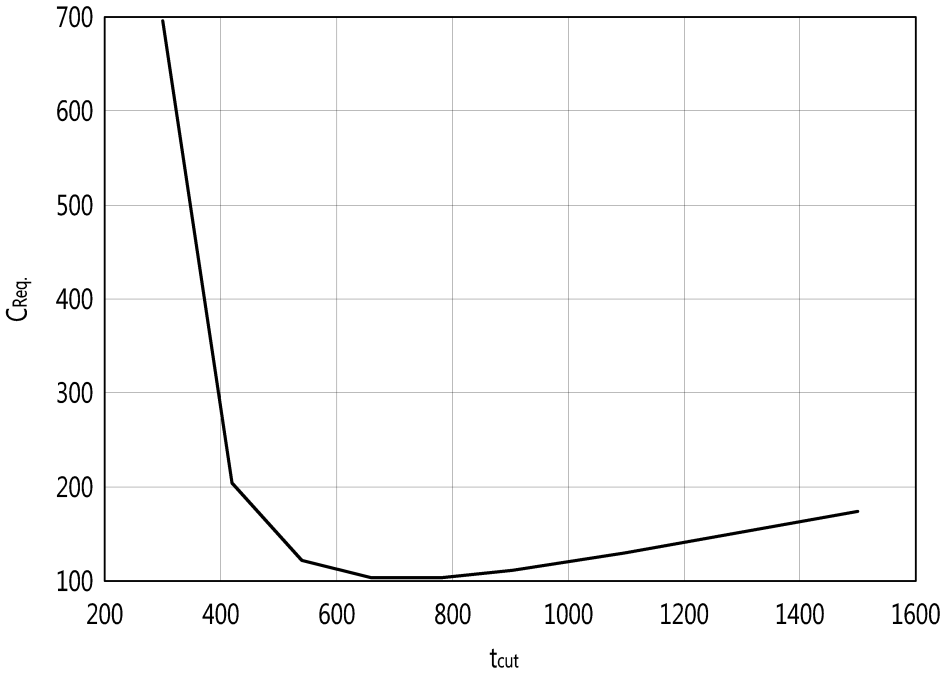
도면5


50
45
40
35
30
25
20
15
10
5
CReq.
0.55
0.6
0.65
0.7
0.75
0.8
0.85
0.9
0.95
PA

도면6


640
630
620
610
600
590
580
570
560
ET-AS-ICT(second)
0.1
0.15
0.2
0.25
0.3
0.35
0.4
0.45
PA

도면7


700
600
500
400
300
200
100
CReq.
200
400
600
800
1000
1200
1400
1600
tcut