

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)(11) 공개번호 10-2021-0148040
(43) 공개일자 2021년12월07일

- (51) 국제특허분류(Int. Cl.)
G06Q 20/02 (2012.01) G06F 16/906 (2019.01)
G06Q 20/06 (2012.01) G06Q 20/10 (2012.01)
G06Q 20/36 (2012.01) G06Q 20/38 (2012.01)
- (52) CPC특허분류
G06Q 20/02 (2013.01)
G06F 16/906 (2019.01)
- (21) 출원번호 10-2021-0163928(분할)
(22) 출원일자 2021년11월25일
심사청구일자 2021년11월25일
(62) 원출원 특허 10-2020-0031905
원출원일자 2020년03월16일
심사청구일자 2020년03월16일
- (30) 우선권주장
1020200007996 2020년01월21일 대한민국(KR)
- (71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
- (72) 발명자
허준범
서울특별시 성북구 안암로 145(안암동5가)
이진희
서울특별시 종로구 평창11길 3-8(평창동)
김민재
서울특별시 동대문구 왕산로 86, 오피스텔동 131
2호(용두동, 동대문 푸르지오시티)
- (74) 대리인
이대호, 박건홍

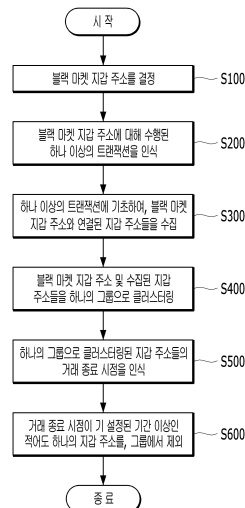
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 암호화폐 지갑 주소의 클러스터링 방법

(57) 요약

본 개시의 일 실시예에 따른, 컴퓨터 판독가능 저장매체에 저장된 컴퓨터 프로그램이 개시된다. 상기 컴퓨터 프로그램은 프로세서로 하여금 이하의 단계들을 수행하게 하기 위한 명령들을 포함하며, 상기 단계들은: 블랙 마켓 지갑 주소를 결정하는 단계; 상기 블랙 마켓 지갑 주소에 대해 수행된 하나 이상의 트랜잭션을 인식하는 단계; 상기 하나 이상의 트랜잭션에 기초하여, 상기 블랙 마켓 지갑 주소와 연결된 지갑 주소들을 수집하는 단계; 및 상기 블랙 마켓 지갑 주소 및 상기 지갑 주소들을 하나의 그룹으로 클러스터링 하는 단계; 를 포함할 수 있다.

대표도 - 도8



(52) CPC특허분류

G06Q 20/065 (2013.01)

G06Q 20/10 (2013.01)

G06Q 20/36 (2013.01)

G06Q 20/382 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711096969
과제번호	2019-0-01697-001
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보보호 핵심원천 기술개발
연구과제명	블록체인 플랫폼 보안취약점 자동분석 기술 개발
기 여 율	1/2
과제수행기관명	고려대 산학협력단
연구기간	2019.06.01 ~ 2020.02.29

이 발명을 지원한 국가연구개발사업

과제고유번호	1711080933
과제번호	2018-0-00269-002
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기술진흥센터
연구사업명	정보통신 방송기술개발
연구과제명	개인정보를 안전하고 편리하게 빅데이터 처리할 수 있는 방법
기 여 율	1/2
과제수행기관명	고려대 산학협력단
연구기간	2020.01.01 ~ 2020.12.31

명세서

청구범위

청구항 1

컴퓨터 판독가능 저장매체에 저장된 컴퓨터 프로그램으로서, 상기 컴퓨터 프로그램은 프로세서로 하여금 이하의 단계들을 수행하게 하기 위한 명령들을 포함하며, 상기 단계들은:

웹 크롤러(Web Crawler)를 이용하여 블랙 마켓과 관련된 웹 페이지에 암호화폐 지갑 주소를 포함하고 있는지 여부를 특정 규칙을 가진 문자열의 집합을 표현하는 정규 표현식(Regular Expression)에 기초하여 인식하는 단계;

상기 웹 페이지에 상기 암호화폐 지갑 주소가 존재하는 경우, 상기 암호화폐 지갑 주소를 블랙 마켓 지갑 주소로 결정하는 단계;

상기 블랙 마켓 지갑 주소에 대해 수행된 하나 이상의 트랜잭션을 인식하는 단계;

상기 하나 이상의 트랜잭션에 기초하여, 상기 블랙 마켓 지갑 주소와 연결된 지갑 주소들을 수집하는 단계; 및

상기 블랙 마켓 지갑 주소 및 상기 지갑 주소들을 하나의 그룹으로 클러스터링 하는 단계;

를 포함하는,

컴퓨터 판독가능한 저장매체에 저장된 컴퓨터 프로그램.

청구항 2

제 1 항에 있어서,

상기 블랙 마켓 지갑 주소를 결정하는 단계는,

지갑 주소와 관련된 입금 트랜잭션과 상기 지갑 주소와 관련된 출금 트랜잭션 사이의 시간 간격, 상기 지갑 주소와 관련된 트랜잭션의 수, 상기 지갑 주소의 잔고에 대한 정보 또는 출금 트랜잭션들 간의 시간 간격 중 적어도 하나에 기초하여 상기 블랙 마켓 지갑 주소를 결정하는 단계;

를 포함하는,

컴퓨터 판독가능한 저장매체에 저장된 컴퓨터 프로그램.

청구항 3

제 1 항에 있어서,

상기 블랙 마켓 지갑 주소를 결정하는 단계는,

상기 웹 크롤러를 이용하여 수집된 지갑 주소와, 하나 이상의 다른 지갑 주소가 결합되어 생성된 출금 트랜잭션을 인식하는 단계; 및

상기 출금 트랜잭션에 포함된, 상기 웹 크롤러를 이용하여 수집된 상기 지갑 주소 및 상기 하나 이상의 다른 지갑 주소 각각을 상기 블랙 마켓 지갑 주소로 결정하는 단계;

를 포함하는,

컴퓨터 판독가능한 저장매체에 저장된 컴퓨터 프로그램.

청구항 4

제 1 항에 있어서,
 상기 하나 이상의 트랜잭션에 기초하여, 상기 블랙 마켓 지갑 주소와 연결된 지갑 주소들을 수집하는 단계는,
 상기 하나 이상의 트랜잭션으로부터 파생된 하나 이상의 파생 트랜잭션을 인식하는 단계; 및
 상기 파생 트랜잭션 각각에 포함된 하나 이상의 지갑 주소를 상기 연결된 지갑 주소들로 수집하는 단계;
 를 포함하는,
 컴퓨터 판독가능 저장매체에 저장된 컴퓨터 프로그램.

청구항 5

제 4 항에 있어서,
 상기 하나 이상의 트랜잭션에 기초하여, 상기 블랙 마켓 지갑 주소와 연결된 지갑 주소들을 수집하는 단계는,
 상기 파생 트랜잭션 각각에 포함된 하나 이상의 지갑 주소 각각이, 하나 이상의 다른 지갑 주소와 결합되어 생성된 출금 트랜잭션을 인식하는 단계; 및
 상기 파생 트랜잭션에 포함된 상기 하나 이상의 지갑 주소 및 상기 하나 이상의 다른 지갑 주소 각각을 상기 연결된 지갑 주소들로 수집하는 단계;
 를 더 포함하는,
 컴퓨터 판독가능한 저장매체에 저장된 컴퓨터 프로그램.

청구항 6

제 1 항에 있어서,
 상기 하나 이상의 트랜잭션에 기초하여, 상기 블랙 마켓 지갑 주소와 연결된 지갑 주소들은,
 암호화폐 믹싱(Mixing) 서비스와 관련된 믹싱 서비스 지갑 주소의 특징을 이용하여 수집되는,
 컴퓨터 판독가능한 저장매체에 저장된 컴퓨터 프로그램.

청구항 7

제 6 항에 있어서,
 상기 믹싱 서비스 지갑 주소는,
 상기 믹싱 서비스 지갑 주소와 관련된 트랜잭션에 포함되는 금액이 기 설정된 기준과 일치하는 지갑 주소인지 여부에 기초하여 결정되는,
 컴퓨터 판독가능한 저장매체에 저장된 컴퓨터 프로그램.

청구항 8

제 6 항에 있어서,
 상기 블랙 마켓 지갑 주소와 연결된 지갑 주소들은,
 상기 블랙 마켓 지갑 주소로부터 수집된 하나 이상의 트랜잭션과 관련된 지갑 주소 중, 상기 믹싱 서비스 지갑 주소를 제외한 지갑 주소인,

컴퓨터 판독가능한 저장매체에 저장된 컴퓨터 프로그램.

청구항 9

제 1 항에 있어서,

상기 하나의 그룹으로 클러스터링된 상기 지갑 주소들의 거래 종료 시점을 인식하는 단계; 및

상기 거래 종료 시점이 기 설정된 기간 이상인 적어도 하나의 지갑 주소를, 상기 그룹에서 제외시키는 단계;

를 더 포함하는,

컴퓨터 판독가능한 저장매체에 저장된 컴퓨터 프로그램.

청구항 10

프로세서;

메모리; 및

통신부;

를 포함하고,

상기 프로세서는,

웹 크롤러(Web Crawler)를 이용하여 블랙 마켓과 관련된 웹 페이지에 암호화폐 지갑 주소를 포함하고 있는지 여부를 특정 규칙을 가진 문자열의 집합을 표현하는 정규 표현식(Regular Expression)에 기초하여 인식하고,

상기 웹 페이지에 상기 암호화폐 지갑 주소가 존재하는 경우, 상기 암호화폐 지갑 주소를 블랙 마켓 지갑 주소로 결정하고,

상기 블랙 마켓 지갑 주소에 대해 수행된 하나 이상의 트랜잭션을 인식하고, 상기 하나 이상의 트랜잭션에 기초하여, 상기 블랙 마켓 지갑 주소와 연결된 지갑 주소들을 수집하고, 그리고

상기 블랙 마켓 지갑 주소 및 상기 연결된 지갑 주소들을 하나의 그룹으로 클러스터링 하는,

컴퓨팅 장치.

발명의 설명

기술 분야

[0001] 본 개시는 암호 화폐 지갑 주소의 클러스터링 기법에 관한 것으로서, 구체적으로 에스크로우(escrow) 방식으로 불법 거래가 수행되는 블랙 마켓 지갑 주소들을 클러스터링 하는 방법에 관한 것이다.

배경 기술

[0002] 최근, 블록체인 기술에 기반한 암호화폐를 이용한 실물 거래가 증가하고 있다. 그러나 익명성을 기반으로 동작하는 블록체인 기술의 특성 때문에, 암호화폐는 마약 등 금제물의 거래, 자금 세탁 등에 이용될 수 있다. 실제로, 추적이 어려운 블록체인 기술의 특성을 이용하여, 다크웹(Dark Web)의 불법거래나 자금세탁 등의 범죄에 암호화폐가 악용되고 있다.

[0003] 암호화폐(특히 비트코인) 거래 시 동일한 지갑은 여러 주소를 이용하여 비트코인 거래를 수행할 수 있다. 따라서 하나의 주소를 추적하는 것 만으로는 불법거래가 수행되는 지갑 및 그 지갑의 주체에 대한 추적이 불가능하다. 따라서 비트코인 트랜잭션 및 트랜잭션이 수행되는 주소들의 클러스터링을 통하여 불법거래가 수행되는 하나의 지갑을 추적할 수 있게 하는 기술이 필요하다.

선행기술문헌

특허문헌

- [0004] (특허문헌 0001) 대한민국 등록특허 제10-2058683호
(특허문헌 0002) 대한민국 등록특허 제10-2051350호

발명의 내용

해결하려는 과제

- [0005] 본 개시는 전술한 배경기술에 대응하여 안출된 것으로, 구체적으로 에스크로우(escrow) 방식으로 불법 거래가 수행되는 블랙 마켓 지갑 주소들을 클러스터링 하는 방법을 제공하고자 한다.
- [0006] 본 개시의 기술적 과제들은 이상에서 언급한 기술적 과제로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

- [0007] 전술한 바와 같은 과제를 해결하기 위한 본 개시의 일 실시예에 따라, 컴퓨터 판독가능 저장매체에 저장된 컴퓨터 프로그램이 개시된다. 상기 컴퓨터 프로그램은 프로세서로 하여금 이하의 단계들을 수행하게 하기 위한 명령들을 포함하며, 상기 단계들은: 블랙 마켓 지갑 주소를 결정하는 단계; 상기 블랙 마켓 지갑 주소에 대해 수행된 하나 이상의 트랜잭션을 인식하는 단계; 상기 하나 이상의 트랜잭션에 기초하여, 상기 블랙 마켓 지갑 주소와 연결된 지갑 주소들을 수집하는 단계; 및 상기 블랙 마켓 지갑 주소 및 상기 지갑 주소들을 하나의 그룹으로 클러스터링 하는 단계; 를 포함할 수 있다.
- [0008] 또한, 상기 블랙 마켓 지갑 주소를 결정하는 단계는, 지갑 주소와 관련된 입금 트랜잭션과 상기 지갑 주소와 관련된 출금 트랜잭션 사이의 시간 간격, 상기 지갑 주소와 관련된 트랜잭션의 수, 상기 지갑 주소의 잔고에 대한 정보 또는 출금 트랜잭션들 간의 시간 간격 중 적어도 하나에 기초하여 상기 블랙 마켓 지갑 주소를 결정하는 단계; 를 포함할 수 있다.
- [0009] 또한, 상기 블랙 마켓 지갑 주소는, 웹 크롤러(Web Crawler)를 이용하여 수집될 수 있다.
- [0010] 또한, 상기 웹 크롤러는, 상기 블랙 마켓 지갑 주소와 관련된 암호화폐의 지갑 주소의 구조적 특징에 기초하여, 웹 페이지로부터 상기 블랙 마켓 지갑 주소를 수집할 수 있다.
- [0011] 또한, 상기 블랙 마켓 지갑 주소를 결정하는 단계는, 상기 웹 크롤러를 이용하여 수집된 지갑 주소와, 하나 이상의 다른 지갑 주소가 결합되어 생성된 출금 트랜잭션을 인식하는 단계; 및 상기 출금 트랜잭션에 포함된, 상기 웹 크롤러를 이용하여 수집된 상기 지갑 주소 및 상기 하나 이상의 다른 지갑 주소 각각을 상기 블랙 마켓 지갑 주소로 결정하는 단계; 를 포함할 수 있다.
- [0012] 또한, 상기 하나 이상의 트랜잭션에 기초하여, 상기 블랙 마켓 지갑 주소와 연결된 지갑 주소들을 수집하는 단계는, 상기 하나 이상의 트랜잭션으로부터 파생된 하나 이상의 파생 트랜잭션을 인식하는 단계; 및 상기 파생 트랜잭션 각각에 포함된 하나 이상의 지갑 주소를 상기 연결된 지갑 주소들로 수집하는 단계;를 포함할 수 있다.
- [0013] 또한, 상기 하나 이상의 트랜잭션에 기초하여, 상기 블랙 마켓 지갑 주소와 연결된 지갑 주소들을 수집하는 단계는, 상기 파생 트랜잭션 각각에 포함된 하나 이상의 지갑 주소 각각이, 하나 이상의 다른 지갑 주소와 결합되어 생성된 출금 트랜잭션을 인식하는 단계; 및 상기 파생 트랜잭션에 포함된 상기 하나 이상의 지갑 주소 및 상기 하나 이상의 다른 지갑 주소 각각을 상기 연결된 지갑 주소들로 수집하는 단계;를 더 포함할 수 있다.
- [0014] 또한, 상기 하나 이상의 트랜잭션에 기초하여, 상기 블랙 마켓 지갑 주소와 연결된 지갑 주소들은, 암호화폐 믹싱(Mixing) 서비스와 관련된 믹싱 서비스 지갑 주소의 특징을 이용하여 수집될 수 있다.
- [0015] 또한, 상기 믹싱 서비스 지갑 주소는, 트랜잭션에 포함되는 금액이 기 설정된 기준과 일치하는 지갑 주소인지 여부에 기초하여 결정될 수 있다.

- [0016] 또한, 상기 블랙 마켓 지갑 주소와 연결된 지갑 주소들은, 상기 블랙 마켓 지갑 주소로부터 수집된 하나 이상의 트랜잭션과 관련된 지갑 주소 중, 상기 암호화폐 믹싱 서비스와 관련된 지갑 주소를 제외한 지갑 주소일 수 있다.
- [0017] 또한, 상기 하나의 그룹으로 클러스터링된 상기 지갑 주소들의 거래 종료 시점을 인식하는 단계; 및 상기 거래 종료 시점이 기 설정된 기간 이상인 적어도 하나의 지갑 주소를, 상기 그룹에서 제외시키는 단계; 를 더 포함할 수 있다.
- [0018] 전술한 바와 같은 과제를 해결하기 위한 본 개시의 일 실시예에 따라, 컴퓨팅 장치가 개시된다. 상기 컴퓨팅 장치는: 프로세서; 메모리; 및 통신부; 를 포함하고, 상기 프로세서는, 블랙 마켓 지갑 주소를 결정하고, 상기 하나 블랙 마켓 지갑 주소 각각에 대해 수행된 하나 이상의 트랜잭션을 인식하고, 상기 하나 이상의 트랜잭션에 기초하여, 상기 블랙 마켓 지갑 주소와 연결된 지갑 주소들을 수집하고, 상기 블랙 마켓 지갑 주소 및 상기 연결된 지갑 주소들을 하나의 그룹으로 클러스터링 할 수 있다.
- [0019] 본 개시에서 얻을 수 있는 기술적 해결 수단은 이상에서 언급한 해결 수단들로 제한되지 않으며, 언급하지 않은 또 다른 해결 수단들은 아래의 기재로부터 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

발명의 효과

- [0020] 본 개시는 암호화폐 지갑 주소의 클러스터링 기법을 제공함으로써, 블랙 마켓에 의하여 운영되는 다수의 암호화폐 지갑 주소를 효율적으로 파악할 수 있도록 한다.
- [0021] 본 개시에서 얻을 수 있는 효과는 이상에서 언급한 효과로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

- [0022] 다양한 양상들이 이제 도면들을 참조로 기재되며, 여기서 유사한 참조 번호들은 총괄적으로 유사한 구성요소들을 지칭하는데 이용된다. 이하의 실시예에서, 설명 목적을 위해, 다수의 특정 세부사항들이 하나 이상의 양상들의 총체적 이해를 제공하기 위해 제시된다. 그러나, 그러한 양상(들)이 이러한 구체적인 세부사항들 없이 실시될 수 있음은 명백할 것이다.
- 도 1은 본 개시의 몇몇 실시예에 따른 암호화폐 지갑 주소 클러스터링을 수행하기 위한 시스템에 대한 일례를 나타낸 도면이다.
- 도 2는 본 개시의 몇몇 실시예에 따른 컴퓨팅 장치의 구성을 나타낸 블록도이다.
- 도 3은 본 개시의 몇몇 실시예에 따른 블랙 마켓 지갑 주소의 거래 및 잔고 현황을 나타낸 도면이다.
- 도 4는 본 개시에 따른 블랙 마켓 지갑 주소의 입출금 현황을 나타낸 도면이다.
- 도 5는 본 개시의 몇몇 실시예에 따른 웹 크롤러가 이용하여 블랙 마켓 지갑 주소를 수집하는 웹 페이지의 일례를 나타낸 도면이다.
- 도 6은 본 개시의 몇몇 실시예에 따른 트랜잭션 및 파생 트랜잭션을 나타낸 도면이다.
- 도 7은 본 개시의 몇몇 실시예에 따른 믹싱 서비스를 표현하기 위한 도면이다.
- 도 8은 본 개시의 몇몇 실시예에 따른 프로세서가 블랙 마켓 지갑 주소를 클러스터링 하는 것을 나타낸 순서도이다.
- 도 9는 본 개시의 몇몇 실시예에 따른 프로세서가 제 1 블랙 마켓 지갑 주소를 결정하는 것을 나타낸 순서도이다.
- 도 10은 본 개시의 몇몇 실시예에 따른 프로세서가 블랙 마켓 지갑 주소와 연결된 지갑 주소들을 수집하는 것을 나타낸 순서도이다.
- 도 11은 본 개시의 몇몇 실시예에 따른 프로세서가 블랙 마켓 지갑 주소와 연결된 지갑 주소들을 수집하는 것을 나타낸 순서도이다.

도 12는 본 개시의 몇몇 실시예들이 구현될 수 있는 예시적인 컴퓨팅 환경에 대한 간략하고 일반적인 개략도를 도시한다.

발명을 실시하기 위한 구체적인 내용

- [0023] 다양한 실시예들 및/또는 양상들이 이제 도면들을 참조하여 개시된다. 하기 설명에서는 설명을 목적으로, 하나 이상의 양상들의 전반적 이해를 돕기 위해 다수의 구체적인 세부사항들이 개시된다. 그러나, 이러한 양상(들)은 이러한 구체적인 세부사항들 없이도 실행될 수 있다는 점 또한 본 개시의 기술 분야에서 통상의 지식을 가진 자에게 감지될 수 있을 것이다. 이후의 기재 및 첨부된 도면들은 하나 이상의 양상들의 특정한 예시적인 양상들을 상세하게 기술한다. 하지만, 이러한 양상들은 예시적인 것이고 다양한 양상들의 원리들에서의 다양한 방법들 중 일부가 이용될 수 있으며, 기술되는 설명들은 그러한 양상들 및 그들의 균등물들을 모두 포함하고자 하는 의도이다. 구체적으로, 본 명세서에서 사용되는 "실시예", "예", "양상", "예시" 등은 기술되는 임의의 양상 또는 설계가 다른 양상 또는 설계들보다 양호하다거나, 이점이 있는 것으로 해석되지 않을 수도 있다.
- [0024] 이하, 도면 부호에 관계없이 동일하거나 유사한 구성 요소는 동일한 참조 번호를 부여하고 이에 대한 중복되는 설명은 생략한다. 또한, 본 명세서에 개시된 실시예를 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 명세서에 개시된 실시예의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다. 또한, 첨부된 도면은 본 명세서에 개시된 실시예를 쉽게 이해할 수 있도록 하기 위한 것일 뿐, 첨부된 도면에 의해 본 명세서에 개시된 기술적 사상이 제한되지 않는다.
- [0025] 본 명세서에서 사용된 용어는 실시예들을 설명하기 위한 것이며 본 발명을 제한하고자 하는 것은 아니다. 본 명세서에서, 단수형은 문구에서 특별히 언급하지 않는 한 복수형도 포함한다. 명세서에서 사용되는 "포함한다(comprises)" 및/또는 "포함하는(comprising)"은 언급된 구성요소 외에 하나 이상의 다른 구성요소의 존재 또는 추가를 배제하지 않는다.
- [0026] 비록 제1, 제2 등이 다양한 소자나 구성요소들을 서술하기 위해서 사용되나, 이들 소자나 구성요소들은 이들 용어에 의해 제한되지 않음은 물론이다. 이들 용어들은 단지 하나의 소자나 구성요소를 다른 소자나 구성요소와 구별하기 위하여 사용하는 것이다. 따라서, 이하에서 언급되는 제1 소자나 구성요소는 본 발명의 기술적 사상 내에서 제2 소자나 구성요소 일 수도 있음은 물론이다.
- [0027] 다른 정의가 없다면, 본 명세서에서 사용되는 모든 용어(기술 및 과학적 용어를 포함)는 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 공통적으로 이해될 수 있는 의미로 사용될 수 있을 것이다. 또 일반적으로 사용되는 사전에 정의되어 있는 용어들은 명백하게 특별히 정의되어 있지 않는 한 이상적으로 또는 과도하게 해석되지 않는다.
- [0028] 더불어, 용어 "또는"은 배타적 "또는"이 아니라 내포적 "또는"을 의미하는 것으로 의도된다. 즉, 달리 특정되지 않거나 문맥상 명확하지 않은 경우에, "X는 A 또는 B를 이용한다"는 자연적인 내포적 치환 중 하나를 의미하는 것으로 의도된다. 즉, X가 A를 이용하거나; X가 B를 이용하거나; 또는 X가 A 및 B 모두를 이용하는 경우, "X는 A 또는 B를 이용한다"가 이들 경우들 어느 것으로도 적용될 수 있다. 또한, 본 명세서에 사용된 "및/또는"이라는 용어는 열거된 관련 아이템들 중 하나 이상의 아이템의 가능한 모든 조합을 지칭하고 포함하는 것으로 이해되어야 한다.
- [0029] 더불어, 본 명세서에서 사용되는 용어 "정보" 및 "데이터"는 종종 서로 상호교환 가능하도록 사용될 수 있다.
- [0030] 이하, 도면 부호에 관계없이 동일하거나 유사한 구성 요소는 동일한 참조 번호를 부여하고 이에 대한 중복되는 설명은 생략한다. 또한, 본 명세서에 개시된 실시예를 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 명세서에 개시된 실시예의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다. 또한, 첨부된 도면은 본 명세서에 개시된 실시예를 쉽게 이해할 수 있도록 하기 위한 것일 뿐, 첨부된 도면에 의해 본 명세서에 개시된 기술적 사상이 제한되지 않는다.
- [0031] 비록 제1, 제2 등이 다양한 소자나 구성요소들을 서술하기 위해서 사용되나, 이들 소자나 구성요소들은 이들 용어에 의해 제한되지 않음은 물론이다. 이들 용어들은 단지 하나의 소자나 구성요소를 다른 소자나 구성요소와 구별하기 위하여 사용하는 것이다. 따라서, 이하에서 언급되는 제1 소자나 구성요소는 본 개시의 기술적 사상 내에서 제2 소자나 구성요소 일 수도 있음은 물론이다.
- [0032] 다른 정의가 없다면, 본 명세서에서 사용되는 모든 용어(기술 및 과학적 용어를 포함)는 본 개시가 속하는 기술 분야에서 통상의 지식을 가진 자에게 공통적으로 이해될 수 있는 의미로 사용될 수 있을 것이다. 또 일반적으로

사용되는 사전에 정의되어 있는 용어들은 명백하게 특별히 정의되어 있지 않는 한 이상적으로 또는 과도하게 해석되지 않는다.

- [0033] 이하의 설명에서 사용되는 구성 요소에 대한 접미사 "모듈" 및 "부"는 명세서 작성의 용이함만이 고려되어 부여되거나 혼용되는 것으로서 그 자체로 서로 구별되는 의미 또는 역할을 갖는 것은 아니다.
- [0034] 본 개시의 목적 및 효과, 그리고 그것들을 달성하기 위한 기술적 구성들은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 본 개시를 설명하는데 있어서 공지 기능 또는 구성에 대한 구체적인 설명이 본 개시의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 그리고 후술되는 용어들은 본 개시에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다.
- [0035] 그러나 본 개시는 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있다. 단지 본 실시예들은 본 개시가 완전하도록 하고, 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 개시의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 개시는 청구항의 범주에 의해 정의될 뿐이다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.
- [0037] 도 1은 본 개시의 몇몇 실시예에 따른 암호화폐 지갑 주소 클러스터링을 수행하기 위한 시스템에 대한 일례를 나타낸 도면이다.
- [0038] 도 1에서의 컴퓨팅 장치(100)는 블록체인 네트워크(200)를 이용하여 암호화폐 지갑 주소 클러스터링을 수행하려는 사용자 또는 시스템 관리자와 관련될 수 있다. 즉, 본 개시에 따른 암호화폐 지갑 주소 클러스터링 방법은 시스템 관리 권한을 가진 주체가 컴퓨팅 장치(100)를 이용함으로써 수행될 수 있다. 나아가, 블록체인 네트워크(200)에 포함된 노드 각각은 관련된 본 개시에 따른 암호화폐 지갑 주소 클러스터링 방법을 수행할 수 있다.
- [0039] 컴퓨팅 장치(100)는 블록체인 네트워크(200)에 포함된 노드로 동작할 수도 있다. 이러한 예시에서, 컴퓨팅 장치(100)는 지갑(wallet) 기능, 마이너(miner) 기능, 및 Full 블록체인 데이터의 저장 기능 중 적어도 하나의 기능을 구현할 수 있다. 예를 들어, 컴퓨팅 장치(100)가 지갑 기능만을 포함하는 경우, 트랜잭션 및 유효성 검증을 수행하는 노드(예컨대, SPV (Simplified Payment Verification)노드)로 동작할 수 있다.
- [0040] 컴퓨팅 장치(100)는 블록체인 네트워크(200)로 쿼리(query) 또는 트랜잭션(transaction)을 발행할 수 있다. 본 개시내용에서의 쿼리는 블록체인 네트워크(200) 상에서 등록된 수신자의 연락처 정보를 조회하는데 사용될 수 있다. 본 개시내용에서의 트랜잭션은 블록체인 네트워크(200) 상에 기록된 데이터에 대한 업데이트(수정/변경/삭제/추가)를 수행하는데 사용될 수 있다.
- [0041] 컴퓨팅 장치(100)는 프로그래밍 언어로 작성된 애플리케이션 소스를 송수신할 수 있다. 예를 들어, 컴퓨팅 장치(100)는 애플리케이션 소스를 컴파일링하여 클라이언트 애플리케이션을 생성할 수 있다. 예를 들어, 생성된 클라이언트 애플리케이션은 블록체인 네트워크(200) 중 적어도 하나로 전달된 후 실행될 수 있다.
- [0042] 컴퓨팅 장치(100)는 디스플레이부(미도시)를 구비하고 있어서, 암호화폐 지갑 주소 클러스터링과 관련된 정보 및 신호를 송수신하는데 있어서 사용자 입력을 수신하고 사용자에게 임의의 형태의 출력을 제공할 수 있다.
- [0043] 본 개시의 몇몇 실시예에서, 블록체인 네트워크(200)는 블록체인 기술에 기반하여 동작하는 복수의 노드들을 의미할 수 있다. 여기서, 블록체인 기술은 블록이 체인형태로 연결된 저장 구조를 사용하여, 관리 대상이 되는 데이터를 블록체인 네트워크에 포함된 복수의 노드들에 저장하는 분산 저장 기술이다.
- [0044] 블록체인 네트워크(200)는 컴퓨팅 장치(100)로부터 전달된 트랜잭션을 사전 결정된 합의 알고리즘에 기초하여 블록 형태로 저장할 수 있다. 블록 형태로 저장되는 데이터는 블록체인 네트워크(200)에 포함된 복수의 노드들에 의해 공유될 수 있다.
- [0045] 블록체인 네트워크(200)는, 구현 형태에 따라서, 임의의 노드들이 합의 동작을 수행할 수 있는 Public 블록체인 네트워크 또는 사전 결정된 노드만이 합의 동작을 수행할 수 있는 Private 블록체인 네트워크를 포함할 수 있다.
- [0046] 본 개시내용의 몇몇 실시예에 따른 블록체인 네트워크(200)에서 수행되는 합의 알고리즘은: PoW(Proof of Work) 알고리즘, PoS(Proof of Stake) 알고리즘, DPoS(Delegated Proof of Stage) 알고리즘, PBFT(Practical Byzantine Fault Tolerance) 알고리즘, DBFT(Delegated Byzantine Fault Tolerance) 알고리즘,

RBFT(Redundant Byzantine Fault Tolerance) 알고리즘, Sieve 알고리즘, Tendermint 알고리즘, Paxos 알고리즘, Raft 알고리즘, PoA(Proof of Authority) 알고리즘 및/또는 PoET(Proof of Elapsed Time) 알고리즘을 포함할 수 있다.

[0047] 본 개시내용의 몇몇 실시예에서, 블록체인 네트워크(200)에서의 노드들은 계층 구조에 따른 블록체인 코어 패키지에 의해 동작할 수 있다. 상기 계층 구조는: 블록체인 네트워크(200)에서 다뤄지는 데이터의 구조를 정의하고 데이터를 관리하는 데이터 계층, 블록의 유효성을 검증하고 블록을 생성하는 마이닝을 수행하고 마이닝 과정에서 채굴자에게 지급되는 수수료의 처리를 담당하는 합의 계층, 스마트 컨트랙트를 처리 및 실행시키는 실행 계층, P2P 네트워크 프로토콜, 해시 함수, 전자서명, 인코딩 및 공통 저장소를 구현 및 관리하는 공통 계층, 및 다양한 어플리케이션이 생성, 처리 및 관리되는 응용 계층을 포함할 수 있다.

[0048] 컴퓨팅 장치(100)는 통신 네트워크(300)를 통하여 블록체인 네트워크(200)에 포함된 적어도 하나의 다른 노드와 통신하기 위한 매커니즘을 가지며, 상기 암호화페 지갑 주소 클러스터링을 수행하기 위한 시스템에서의 임의의 형태의 노드를 의미할 수 있다. 예를 들어, 컴퓨팅 장치(100)는 마이크로프로세서, 메인프레임 컴퓨터, 디지털 프로세서, 휴대용 디바이스, PC(Personal Computer), 랩탑 컴퓨터, 워크스테이션 및/또는 네트워크 접속성을 갖는 임의의 전자 디바이스를 포함할 수 있다. 또한, 컴퓨팅 장치(100)는 에이전트(Agent), API(Application Programming Interface) 및 플러그-인(Plug-in) 중 적어도 하나에 의해 구현되는 임의의 서버를 포함할 수도 있다. 또한, 컴퓨팅 장치(100)는 애플리케이션 소스 및/또는 클라이언트 애플리케이션을 포함할 수 있다.

[0049] 컴퓨팅 장치(100)는 프로세서(110), 메모리 및 통신부를 포함하여, 임의의 데이터를 처리 및 저장할 수 있는 임의의 블록체인 네트워크(200)에 포함된 컴퓨팅 장치일 수 있다.

[0050] 본 개시내용의 일 실시예에 따른 통신 네트워크(300)는 공중전화 교환망(PSTN:Public Switched Telephone Network), xDSL(x Digital Subscriber Line), RADSL(Rate Adaptive DSL), MDSL(Multi Rate DSL), VDSL(Very High Speed DSL), UADSL(Universal Asymmetric DSL), HDSL(High Bit Rate DSL) 및 근거리 통신망(LAN) 등과 같은 다양한 유선 통신 시스템들을 사용할 수 있다.

[0051] 또한, 본 개시내용에서 제시되는 통신 네트워크(300)는 CDMA(Code Division Multi Access), TDMA(Time Division Multi Access), FDMA(Frequency Division Multi Access), OFDMA(Orthogonal Frequency Division Multi Access), SC-FDMA(Single Carrier-FDMA) 및 다른 시스템들과 같은 다양한 무선 통신 시스템들을 사용할 수 있다. 본 개시내용에서 설명된 기술들은 위에서 언급된 네트워크들뿐만 아니라, 임의의 형태의 다른 통신 네트워크들에서도 사용될 수 있다.

[0053] 도 2는 본 개시의 몇몇 실시예에 따른 컴퓨팅 장치의 블록도이다.

[0054] 도 2에서 도시되는 바와 같이, 컴퓨팅 장치(100)는 프로세서(110), 메모리(120) 및 통신부(미도시)를 포함할 수 있다.

[0055] 프로세서(110)는 하나 이상의 코어로 구성될 수 있으며, 컴퓨팅 장치의 중앙 처리 장치(CPU: central processing unit), 범용 그래픽 처리 장치(GPGPU: general purpose graphics processing unit), 텐서 처리 장치(TPU: tensor processing unit) 등과 같이 메모리 상에 저장된 명령어들을 실행시킴으로써 블랙 마켓 지갑 주소 클러스터링을 수행하기 위한 임의의 형태의 프로세서를 포함할 수 있다. 프로세서(110)는 메모리에 저장된 컴퓨터 프로그램을 관독하여 본 개시의 몇몇 실시예에 따른 블랙 마켓 지갑 주소 클러스터링을 수행할 수 있다. 프로세서(110)는 블랙 마켓 지갑 주소 클러스터링 방법을 수행하기 위하여 컴퓨팅 장치(100)의 컴포넌트들의 전반적인 동작들을 제어할 수 있다.

[0056] 에스크로 거래관, 구매자와 판매자 간 신용관계가 불확실할 때 제3자가 상거래가 원활히 이루어질 수 있도록 중계를 하는 매매 보호 서비스를 의미한다.

[0057] 특히 전자 상거래 서비스에 있어서는 전자상거래의 경우에는 '결제대금 예치'를 의미하며, 거래대금을 제3자에게 맡긴 뒤 물품 배송을 확인하고 판매자에게 지불하는 제도로 사용되고 있다. 구체적으로 에스크로 서비스는, 소비자가 물건 값을 은행 등 공신력 있는 제3자에게 보관한 뒤, 배송이 정상적으로 완료되면 은행에서 판매자에게로 입금하는 방식으로 운영될 수 있다.

[0058] 블록체인 기술을 기반으로 하는 암호화폐에서의 지갑은 블록체인 네트워크와 상호 작용하는 수단 중 하나일 수 있다. 지갑은 실제로 암호화폐를 저장하지 않으며, 다만 지갑은 블록체인 트랜잭션을 통해 암호화폐를 주고받을

때 필요한 정보를 생성할 수 있다. 이러한 정보는 하나 또는 그 이상의 공개 키와 개인 키 쌍으로 구성될 수 있다.

- [0059] 지갑에는 또한 공개 키와 개인 키를 기반으로 생성되는 영숫자 식별자인 공개 주소가 포함될 수 있으며, 이러한 주소는 코인이 전송될 수 있는 블록체인 상의 특정한 “위치”를 의미할 수 있다. 따라서, 특정 주체는 자금을 전달받기 위해 공개 주소를 공유할 수 있다. 자금의 이동은 한 주소에서 다른 주소로 암호 화폐가 전송됨으로써 이루어질 수 있다.
- [0060] 본 개시에 따른 프로세서(110)는, 불법거래나 자금세탁에 이용되는 것으로 의심되는 블랙 마켓 지갑 주소를 결정할 수 있다.
- [0061] 구체적으로, 이러한 블랙 마켓 지갑 주소는, 불법거래 등이 주로 이루어지는 다크 웹에 공개된 주소를 기초로 결정될 수 있다.
- [0062] 예를 들어, 프로세서(110)는, 웹 크롤러(Web Crawler) 등, 다크 웹 상에서 불법 거래를 위해 공개된 암호화폐 지갑 주소를 인식하는 프로그램을 이용하여, 다크 웹 내에 공개된 불법 거래용 주소에 대한 데이터를 수집할 수 있다.
- [0063] 또한, 프로세서(110)는 수집된 불법 거래용 주소 데이터를 블랙 마켓 지갑 주소로 결정하고, 이와 연결된 지갑 주소들을 인식할 수 있다. 본 개시에 있어서, 프로세서(110)는 상기 블랙 마켓 지갑 주소와 연결된 지갑 주소들을 클러스터링하여 하나의 그룹을 형성할 수 있다.
- [0064] 상기 웹 크롤러 등, 상기 지갑 주소를 인식하는 프로그램은 메모리(120)에 미리 저장되어, 프로세서(110)에 의해 실행될 수 있다.
- [0066] 통신부(미도시)는 네트워크 접속을 위한 유/무선 인터넷 모듈을 포함할 수 있다. 통신부(미도시)는 블록체인 네트워크(200)에 포함된 노드 중 적어도 하나와의 통신을 수행할 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. 유선 인터넷 기술로는 XDSL(Digital Subscriber Line), FTTH(Fibers to the home), PLC(Power Line Communication) 등이 이용될 수 있다.
- [0067] 전술한 컴포넌트들은 예시적인 것으로서 본 개시내용의 권리범위가 전술한 컴포넌트들로 제한되지는 않는다. 즉, 본 개시내용의 실시예들에 대한 구현 양태에 따라서 추가적인 컴포넌트들이 포함되거나 또는 전술한 컴포넌트들 중 일부가 생략될 수 있다.
- [0068] 컴퓨팅 장치(100)는 메모리(120)를 더 포함할 수 있다. 메모리는 프로세서(110)의 동작을 위한 프로그램을 저장할 수 있고, 입/출력되는 데이터들을 임시 또는 영구 저장할 수도 있다. 메모리는 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. 이러한 메모리는 프로세서에 제어에 의하여 동작될 수 있다.
- [0070] 도 3은 본 개시에 따른 블랙 마켓 지갑 주소의 거래 및 잔고 현황을 나타낸 도면이다.
- [0071] 도 3을 참조하면, 블랙 마켓 지갑 주소로 결정된 믹싱 서비스 지갑 주소의 거래 현황을 볼 수 있다. 상술한 바와 같이, 블랙 마켓에서 불법 거래에 이용되는 지갑 주소에서는 입금된 금액이 믹싱을 위해 그대로 다른 계좌로 출금하는 행위가 반복적으로 이루어진다.
- [0072] 따라서, 36회의 거래가 발생(Transactions, 36)하였음에도 불구하고, 입금된 전체 금액(Total Received)과 출금된 전체 금액(Total Sent)이 동일함을 볼 수 있다.
- [0073] 프로세서(110)는 도 3에 도시된 바와 같은 전체적인 금액의 출입현황 뿐만 아니라, 다양한 요소를 고려하여 블랙 마켓 지갑 주소를 결정할 수 있는데, 이는 이하 후술한다.
- [0074] 블록체인 기술을 기반으로 하는 암호화폐에서의 지갑(400)은 블록체인 네트워크와 상호 작용하는 수단 중 하나

일 수 있다. 지갑은 실제로 암호화폐를 저장하지 않으며, 다만 지갑은 블록체인 트랜잭션을 통해 암호화폐를 주고받을 때 필요한 정보를 생성할 수 있다. 이러한 정보는 하나 또는 그 이상의 공개 키와 개인 키 쌍으로 구성될 수 있다.

- [0075] 즉, 암호화폐 지갑(400)은 블록체인 분산원장에 기록되는 거래 트랜잭션 데이터를 생성하고 서명하는 일에 사용되는 비공개 키를 보관하고 관리하기 위한 도구를 의미할 수 있다.
- [0076] 지갑에는 또한 공개 키와 개인 키를 기반으로 생성되는 영수증 식별자인 공개 주소가 포함될 수 있으며, 이러한 주소는 코인이 전송될 수 있는 블록체인 상의 특정한 “위치”를 의미할 수 있다. 따라서, 특정 주체는 자금을 전달받기 위해 공개 주소를 공유할 수 있다. 자금의 이동은 한 주소에서 다른 주소로 암호 화폐가 전송됨으로써 이루어질 수 있다.
- [0077] 도 3을 참조하면, 본 개시에 따른 암호화폐 지갑(400)은 지갑 주소(410), 해당 지갑에 대해 수행된 트랜잭션 수(420), 트랜잭션을 통해 입금된 전체 금액(430), 출금된 전체 금액(440) 및 잔액(450) 정보와 관련될 수 있다.
- [0078] 블록체인 네트워크(200) 상에 개별 암호화폐 지갑(400)에 대해 수행된 트랜잭션에 관한 정보가 모두 기록되기 때문에, 상기 정보들(410 내지 450)은 블록 익스플로러(BlockExplorer)와 같은 인터넷 사이트를 통하여 쉽게 조회될 수 있다.
- [0079] 이하 구체적으로 설명한다.
- [0080] 본 개시에 있어 지갑 주소(410)는 블록체인 네트워크 상에 기록되는 트랜잭션에 기초하여, 암호화폐를 전송하는데 사용되는 일련의 문자 및 숫자로 구성된 데이터를 의미할 수 있다.
- [0081] 본 개시에 있어 지갑 주소(410)는 좌측의 QR 코드와 연동될 수 있다.
- [0082] 암호화폐 지갑(400)은 당해 암호화폐 지갑(400)에 대해 수행된 전체 트랜잭션의 수(420)와 연관될 수 있다. 따라서, 프로세서(110)는 블록체인 거래 정보를 기록하는 사이트로부터 상기 암호화폐 지갑(400)에 대한 트랜잭션 수 정보를 조회할 수 있다.
- [0083] 프로세서(110)는 통신부(미도시)를 통해 상기 블록체인 거래 정보를 기록하는 인터넷 사이트로부터 상기 암호화폐 지갑(400)이 다른 암호화폐 지갑으로부터 입금된 전체 금액(430)을 조회할 수 있다.
- [0084] 입금 금액과 마찬가지로, 프로세서(110)는 통신부(미도시)를 통해 상기 블록체인 거래 정보를 기록하는 인터넷 사이트로부터 상기 암호화폐 지갑(400)이 다른 암호화폐 지갑으로 출금한, 출금된 전체 금액(440)을 조회할 수 있다.
- [0085] 프로세서(110)는 통신부(미도시)를 통해 상기 블록체인 거래 정보를 기록하는 인터넷 사이트로부터 상기 암호화폐 지갑(400)의 최종 잔액(450)을 조회할 수 있다.
- [0086] 일반적으로 블랙 마켓에서 이용하는 암호화폐 지갑(400)은 입금된 전체 금액(430)과 출금된 전체 금액(440)이 동일하고, 따라서 잔액(450)이 0일 수 있다. 또한 일반적인 암호화폐 지갑들에 비해 짧은 기간 동안 많은 트랜잭션 수(420)를 갖는다는 특징이 있을 수 있다. 또한 일정 기간 동안 사용된 이후에는 더 이상 사용되지 않는다는 특징을 가질 수 있다.
- [0087] 본 개시에 따른 프로세서(110)는 이와 같은 특징에 기초하여 블랙 마켓에서 사용되는 암호화폐 지갑을 추적할 수 있다. 이하 구체적으로 설명한다.
- [0089] 도 4는 본 개시에 따른 블랙 마켓 지갑 주소의 입출금 현황을 나타낸 도면이다.
- [0090] 도 4를 참조하면, 블랙 마켓 지갑 주소와 관련된 개별 트랜잭션의 구체적인 내역을 확인할 수 있다.
- [0091] 블랙 마켓 지갑 주소에서는 입금된 금액이 그대로 출금되어 다른 계좌로 전송된다. 원 안에 표기된 금액이 출금되기 직전, 그 아래의 트랜잭션에서 해당 지갑 주소에 동일한 금액이 입금된 것을 볼 수 있다.
- [0092] 따라서, 프로세서(110)는 상술된 특징을 가지는 지갑 주소가 블랙 마켓을 운영하는 주체가 이용하는 지갑 주소임을 알 수 있다.
- [0093] 현재 암호화폐 지갑 시스템에 널리 사용되는 계층 결정적 지갑(Hierarchical Deterministic Wallet)의 특성상, 동일한 지갑이라도 서로 다른 트랜잭션에 대해서 다른 주소를 이용할 수 있다. 그러나, 블랙 마켓의 특성

상, 구매자와 판매자에 의한 트랜잭션을 제외하면, 암호화폐는 블랙 마켓 지갑들 사이에서만 전송될 가능성이 높다. 따라서, 프로세서(110)는 하나의 블랙 마켓 지갑 주소의 트랜잭션 내역을 기점으로, 연결된 트랜잭션을 추적하여 복수의 상기 블랙 마켓 지갑 주소와 연결된 지갑 주소들을 클러스터링하여 하나의 지갑에 대응시킬 수 있다.

- [0094] 도 4는 프로세서(110)에 의해 조회된, 임의의 암호화폐 지갑(400)에 대해 수행된 트랜잭션 내역(500)을 도시한다.
- [0095] 도 4에서 도시되는 트랜잭션 내역(500)은 암호화폐 지갑(400)에 대해 수행된 트랜잭션의 일부만을 도시한다. 또한 도 4에서 도시되는 트랜잭션 수행 양상은 암호화폐 지갑(400)에 대해 수행되는 트랜잭션 생성의 일 양상에 불과하다.
- [0096] 프로세서(110)는 메모리(120)에 기 저장된, 블랙 마켓 지갑 주소들의 특징들을 인식할 수 있다. 따라서, 프로세서(110)는 암호화폐 지갑(400)에 대해 수행되는 트랜잭션의 다양한 특징이 블랙 마켓 지갑 주소들의 특징들에 대응되는지 여부를 인식할 수 있다. 이에 기초하여, 프로세서(110)는 암호화폐 지갑(400)이 블랙 마켓에 의하여 운영되는 암호화폐 지갑에 해당하는 지 여부를 판단할 수 있다.
- [0097] 도 4를 참조하면, 트랜잭션 내역(500)은 트랜잭션 발생 시간(511, 512), 출금 금액(521), 입금 금액(522), 입금 트랜잭션(531), 출금 트랜잭션(532)을 포함할 수 있다.
- [0098] 이하 구체적으로 각각 설명한다.
- [0099] 임의의 암호화폐 지갑과 관련하여, 트랜잭션 내역(500)은 입금 트랜잭션을 포함할 수 있다. 도 4에 도시된 입금 트랜잭션(531)은 하나의 지갑 주소로부터 복수의 지갑 주소에 대한 암호화폐의 전송이 수행되었음을 보여준다. 입금 트랜잭션(531)에서, 트랜잭션 중앙에 위치한 화살표 좌측에 나열된 하나의 지갑 주소로부터 약 17.33 BTC의 비트코인이 화살표 우측에 나열된 복수의 지갑 주소로 분배되어 송금되었다. 이 중, 트랜잭션 내역(500)과 관련된 지갑 주소는 화살표 우측에 나열된 복수의 지갑 주소 중 아래에서 3번째에 위치한 지갑 주소이며, 당해 지갑 주소로 0.00306600 BTC의 비트코인이 입금되었음을 확인할 수 있다.
- [0100] 일반적인 암호 화폐의 전송은 하나의 지갑으로부터 하나의 지갑으로 이루어질 수 있다. 따라서, 복수의 지갑 주소로 출금이 이루어지는 트랜잭션의 경우, 해당 트랜잭션에 의하여 암호화폐를 입금받는 복수의 지갑 주소들은 동일한 운영 주체에 의하여 소유되는 지갑이라고 볼 수 있다.
- [0101] 또한, 블랙 마켓 지갑 주소들은 구매자와 판매자에 대한 입금 및 출금 외에는 상호 간에만 입출금을 수행한다.
- [0102] 이러한 특징에 기초하면, 하나의 블랙 마켓 지갑 주소로부터 복수의 암호화폐 지갑 주소로 암호화폐의 전송이 이루어진 경우, 암호화폐를 입금받는 복수의 지갑 주소들이 블랙 마켓 지갑 주소와 연결된 지갑 주소라고 판단할 수 있다. 따라서, 프로세서(110)는 상기 연결된 지갑 주소들을 클러스터링 할 수 있다.
- [0103] 또는, 프로세서(110)는 암호화폐를 입금받는 복수의 지갑 주소들을, 클러스터링 작업을 수행하기 위한 시발점이 되는 블랙 마켓 지갑 주소로 결정할 수 있다. 이 경우, 프로세서(110)는 복수의 지갑 주소들 각각에 대하여 본 개시에 따른 클러스터링 기법을 적용하여, 동시에 더 많은 블랙 마켓 지갑 주소들을 발견해낼 수 있다.
- [0104] 이러한 특징을 이용하면, 블랙 마켓 지갑 주소를 단 하나만 특정하더라도 다수의 블랙 마켓 지갑 주소들을 한꺼번에 발견해낼 수 있다. 따라서 블랙 마켓에서 이루어지는 불법 거래 행위의 추적이 용이할 수 있다.
- [0105] 상기 내용을 도 4에 도시된 입금 트랜잭션(531)에 대입하여 본다. 도 4의 입금 트랜잭션(531)에서, 화살표 우측의 복수의 지갑 주소들은 별개의 주소로서 입금이 수행되었으나, 당해 복수의 지갑 주소들은 모두 한 명의 암호화폐 사용자의 소유라고 볼 수 있다.
- [0106] 이러한 특성에 기초하여 프로세서(110)는 복수의 지갑 주소를 블랙 마켓 지갑 주소와 연결된 지갑 주소들로 결정할 수 있다. 이에, 프로세서(110)는 상기 블랙 마켓 지갑 주소 및 연결된 지갑 주소들을 하나의 암호화폐 사용 주체에 대하여 클러스터링 할 수 있다. 즉, 입금 트랜잭션(531)과 같이, 하나의 트랜잭션 내에서 복수의 지갑 주소들에 의해 입금이 수행된 경우, 상기 복수의 지갑 주소들은 하나의 주체에 대해 클러스터링 될 수 있을 것이다.
- [0107] 임의의 암호화폐 지갑과 관련하여, 트랜잭션 내역(500)은 출금 트랜잭션을 포함할 수 있다. 도 4에 도시된 출금 트랜잭션(532)은 복수의 지갑 주소로부터 하나의 지갑 주소에 대한 암호화폐의 전송이 수행되었음을 보여준다. 출금 트랜잭션(532)에서, 트랜잭션 중앙에 위치한 화살표 좌측에 나열된 복수의 지갑 주소로부터 약 0.1137 BTC

의 비트코인이 화살표 우측에 나열된 하나의 지갑 주소로 송금되었다. 이 중, 트랜잭션 내역(500)과 관련된 지갑 주소는 화살표 좌측에 나열된 복수의 지갑 주소 중 위에서 2번째에 위치한 지갑 주소이며, 당해 지갑 주소로 0.00439600 BTC의 비트코인이 입금되었음을 확인할 수 있다.

- [0108] 일반적인 블록체인 및 암호화폐 지갑과 관련된 클라이언트 프로그램들은 복수의 주소가 결합하여 하나의 트랜잭션을 생성할 수 있도록 지원할 수 있다. 그러나, 이러한 클라이언트들은 일반적으로 복수의 사용자들이 하나의 트랜잭션을 생성하는 것을 지원하지 않을 수 있다. 따라서, 복수의 지갑 주소로부터 출금이 이루어지는 트랜잭션의 경우라도 해당 트랜잭션은 한 명의 사용자에 의해 생성된 것이라고 볼 수 있다. 따라서, 이 경우, 출금이 이루어진 복수의 지갑 주소는 한 명의 사용자와 연관된다고 볼 수 있다.
- [0109] 또한, 블랙 마켓 지갑 주소들은 구매자와 판매자에 대한 입금 및 출금 외에는 상호 간에만 입출금을 수행한다.
- [0110] 이러한 특징에 기초하면, 블랙 마켓 지갑 주소를 포함하는 복수의 지갑 주소로부터 하나의 암호화폐 지갑 주소로 암호화폐의 전송이 이루어진 경우, 출금이 이루어진 복수의 지갑 주소들이 블랙 마켓 지갑 주소와 연결된 지갑 주소라고 판단할 수 있다. 따라서, 프로세서(110)는 상기 연결된 지갑 주소들을 클러스터링 할 수 있다.
- [0111] 또는, 프로세서(110)는 암호화폐가 출금되는 복수의 지갑 주소들을, 클러스터링 작업을 수행하기 위한 시발점이 되는 블랙 마켓 지갑 주소로 결정할 수 있다. 이 경우, 프로세서(110)는 복수의 지갑 주소들 각각에 대하여 본 개시에 따른 클러스터링 기법을 적용하여, 동시에 더 많은 블랙 마켓 지갑 주소들을 발견해낼 수 있다.
- [0112] 이러한 특징을 이용하면, 블랙 마켓 지갑 주소를 단 하나만 특정하더라도 다수의 블랙 마켓 지갑 주소들을 한꺼번에 발견해낼 수 있다. 따라서 블랙 마켓에서 이루어지는 불법 거래 행위의 추적이 용이할 수 있다.
- [0113] 상기 내용도 도 4에 도시된 출금 트랜잭션(532)에 대입하여 본다. 도 4의 출금 트랜잭션(532)은 화살표 좌측의 복수의 지갑 주소들에 의해 출금이 수행되었다. 그러나 상술한 바와 같이, 암호화폐 클라이언트의 특성 상 당해 복수의 지갑 주소들은 모두 동일한 블록체인 또는 암호화폐 사용 주체의 소유라고 볼 수 있다.
- [0114] 이러한 특성에 기초하여 프로세서(110)는 복수의 지갑 주소를 블랙 마켓 지갑 주소와 연결된 지갑 주소들로 결정할 수 있다. 이에, 프로세서(110)는 상기 블랙 마켓 지갑 주소 및 연결된 지갑 주소들을 하나의 암호화폐 사용 주체에 대하여 클러스터링 할 수 있다.
- [0115] 즉, 출금 트랜잭션(532)과 같이, 하나의 트랜잭션 내에서 복수의 지갑 주소들에 의해 출금이 수행된 경우, 상기 복수의 지갑 주소들은 한 명의 사용자에 대해 클러스터링 될 수 있을 것이다.
- [0116] 이는 사용자에 대해서 복수의 지갑 주소들을 클러스터링 하기 위한 방법의 하나의 예시일 뿐이므로, 클러스터링 하기 위한 방법은 이에 한정되지 않는다.
- [0117] 트랜잭션 내역(500)에 포함된 개별 트랜잭션들은 해당 트랜잭션이 수행된 시간을 포함할 수 있다. 출금 트랜잭션에 있어서는 출금 시간 정보(512)가, 입금 트랜잭션에 있어서는 입금 시간 정보(512)가 포함될 수 있다.
- [0118] 트랜잭션 내역(500)에 포함된 개별 트랜잭션들은 해당 트랜잭션에 의해 전송된 암호화폐의 양에 관한 정보를 포함할 수 있다.
- [0119] 당해 트랜잭션 내역(500)과 관련된 암호화폐 지갑으로부터 출금이 수행된 경우, 암호화폐의 양 앞에 -가 붙어 표현된다. 당해 트랜잭션 내역(500)과 관련된 암호화폐 지갑에 대해 입금이 수행된 경우, 암호화폐의 양 앞에 +가 붙어 표현된다. 이는 예시적인 표현에 불과하므로, 암호화폐 지갑에 암호화폐가 입금되었는지 출금되었는지를 표현하는 방식은 달라질 수 있다.
- [0120] 도 4를 참조하면, 트랜잭션 내역(500)과 관련된 암호화폐 지갑이 블랙 마켓과 관련되어 있을 경우, 블랙 마켓이 운영하는 암호화폐 지갑의 경우 입금과 출금이 일정한 주기로 반복된다는 특성으로 인해 출금 금액(521) 및 입금 금액(522)이 동일할 수 있다. 따라서, 프로세서(110)는 출금 금액(521)과 입금 금액(522)이 동일한 트랜잭션들이 트랜잭션 내역(500)에 다수 포함되어 있다면, 당해 트랜잭션 내역(500)과 관련된 암호화폐 지갑(400) 및 상기 암호화폐 지갑 주소(410)를 블랙 마켓에 의하여 운영되는 암호화폐 지갑 및 블랙 마켓 지갑 주소로 결정할 수 있다.
- [0121] 다만 이는 블랙 마켓에 의하여 운영되는 암호화폐 지갑 및 블랙 마켓 지갑 주소 주소를 결정하기 위한 고려 요소의 일례에 불과할 뿐이다. 따라서, 블랙 마켓에 의하여 운영되는 암호화폐 지갑 및 그 주소를 결정하기 위한 고려 요소는 이에 한정되지 않는다.

- [0123] 도 5는 본 개시의 몇몇 실시예에 따른 웹 크롤러가 이용하여 블랙 마켓 지갑 주소를 수집하는 웹 페이지의 일례를 나타낸 도면이다.
- [0124] 본 개시에 있어서 웹 크롤러는 인터넷 상에 있는 자료를 가져와 데이터 분석하기 쉬운 형태로 가공하는 작업을 수행하는 모듈을 의미할 수 있다.
- [0125] 예를 들어, 본 개시에 따른 프로세서(110)는 상기 웹 크롤러를 이용하여 블랙 마켓 지갑 주소를 수집할 수 있다. 이하 예를 들어 설명한다.
- [0126] 도 5에서는 제품에 대한 대금을 지급하기 위한 정보를 구매자에게 제공하는 웹 페이지(600)가 도시된다. 이러한 웹 페이지(600)는 인터넷뿐만 아니라, 일반적으로 블랙 마켓이 개설되는 다크 웹(Dark Web) 상에 존재할 수 있다.
- [0127] 웹 페이지(600)는 제품 대금을 수령하기 위한 암호화폐 지갑 주소(610)를 포함할 수 있다.
- [0128] 웹 페이지(600)에 포함된 암호화폐 지갑 주소는 일정한 구조적 특징을 가질 수 있다. 도 5에서 도시되듯, 웹 페이지(600)에 포함된 암호화폐 지갑 주소(610)는 다수의 숫자 및 문자를 포함하는 문자열 형태일 수 있다. 이러한 암호화폐 지갑 주소(610)는 블랙 마켓에서 제품의 대금을 수령하기 위해 이용하는 암호화폐의 종류에 따라 상이할 수 있다. 예를 들면, 예를 들어, 암호화폐의 일종인 비트코인의 경우, 지갑 주소는 1 혹은 3으로 시작하고, a 내지 z, A 내지 Z 및 숫자 0~9로 이루어진 26~33자의 무작위한 문자열이다.
- [0129] 이를 이용하여, 상기 블랙 마켓 지갑 주소와 관련된 암호화폐의 지갑 주소의 구조적 특징에 기초하여, 웹 페이지로부터 상기 블랙 마켓 지갑 주소를 수집할 수 있다. 이하 구체적으로 설명한다.
- [0130] 프로세서(110)는 통신부(미도시) 및 상기 웹 크롤러를 이용하여, 도 5에 도시된 바와 같은 웹 페이지(600)로부터 암호화폐 지갑 주소(610)를 수집할 수 있다. 이하 예를 들어 설명한다.
- [0131] 본 개시의 몇몇 실시예에 따른 웹 크롤러는 조회된 웹 페이지(600)가 암호화폐 지갑 주소(610)를 포함하고 있는지 여부를 정규 표현식(Regular Expression)에 기초하여 인식할 수 있다.
- [0132] 정규 표현식은 특정한 규칙을 가진 문자열의 집합을 표현하는데 사용하는 형식 언어이다. 프로세서(110)는 수집하고자 하는 종류의 암호화폐 지갑 주소가 가지는 규칙에 대응하는 정규 표현식을 이용하여, 웹 페이지(600) 내에 암호화폐 지갑 주소(610)가 존재하는 지 여부를 검색할 수 있다. 웹 페이지(600) 내에 암호화폐 지갑 주소(610)가 존재하는 경우, 프로세서(110)는 이를 수집하여 블랙 마켓 지갑 주소로 결정할 수 있다.
- [0133] 예를 들어, 암호화폐의 일종인 비트코인의 경우, 암호화폐 지갑 주소(610)는 1 혹은 3으로 시작하고, a 내지 z, A 내지 Z 및 숫자 0~9로 이루어진 26~33자의 무작위한 문자열이다. 프로세서(110)는 이러한 규칙을 갖는 문자열이 웹 페이지(600) 내에 존재하는 지를 상기 정규 표현식을 이용해 검색할 수 있다. 이러한 문자열이 존재하는 경우, 프로세서(110)는 해당 문자열을 수집하여 블랙 마켓 지갑 주소로 결정할 수 있다.
- [0135] 도 6은 본 개시의 몇몇 실시예에 따른 트랜잭션 및 파생 트랜잭션을 나타낸 도면이다.
- [0136] 도 6은 트랜잭션 해시 값(de711eaa2707f1d...)을 갖는 트랜잭션의 출금 지갑에서의 제 1 트랜잭션(710a) 및 입금 지갑에서의 제 2 트랜잭션(710b)을 도시한다.
- [0137] 제 1 트랜잭션은 상기 트랜잭션 해시 값을 갖는 트랜잭션의 출금 지갑에서의 양상이며, 제 2 트랜잭션은 상기 트랜잭션 해시 값을 갖는 트랜잭션의 입금 지갑에서의 양상일 수 있다. 본질적으로 제 1 트랜잭션 및 제 2 트랜잭션은 동일한 트랜잭션일 수 있다.
- [0138] 제 1 트랜잭션(710a) 및 제 2 트랜잭션(710b)에 따르면, 지갑 주소(411)에 0.06131465 BTC가 입금되었음을 확인할 수 있다.
- [0139] 본 개시에 있어 파생 트랜잭션(800)은, 암호화폐 지갑 주소로 입금된 이전 트랜잭션에 기초하여 새로이 생성된 트랜잭션을 의미할 수 있다.
- [0140] 예를 들어, 제 2 트랜잭션(710b)에 따르면, 지갑 주소(411)에 0.06131465 BTC가 입금된 것을 확인할 수 있다. 그리고, 당해 지갑 주소(411)는 이미 0.30815704 BTC를 추가적으로 보유하고 있음을 파생 트랜잭션(800)의 화살

표 좌측을 통해 알 수 있다.

- [0141] 지갑 주소(411)와 관련된 주체는, 지갑 주소(411)가 이미 보유하고 있었던 금액과, 제 2 트랜잭션(710b)을 통해 입금된 금액을 결합하여 새로운 트랜잭션을 생성할 수 있으며, 파생 트랜잭션(800)은 그 일례이다.
- [0142] 상술한 바와 같이, 블랙 마켓 지갑 주소들은 서로 간에만 암호화폐를 전송하는 특징을 가지고 있다. 따라서, 파생 트랜잭션에서 입출금이 수행되는 모든 지갑 주소들은 블랙 마켓 지갑 주소와 관련된 주체의 소유일 가능성이 높을 수 있다. 따라서, 프로세서(110)들은 파생 트랜잭션(800)에 포함된 모든 암호화폐 지갑 주소들을 하나의 주체에 대하여 클러스터링 할 수 있다.
- [0144] 도 7은 본 개시의 몇몇 실시예에 따른 믹싱 서비스를 표현하기 위한 도면이다.
- [0145] 본 개시에 있어, 암호화폐 믹싱이란 암호화폐 거래 내역을 뒤섞어버림으로써, 어디에서 암호화폐를 받고, 어디로 암호화폐를 보내는지에 대한 정보를 알 수 없도록 숨기는 기술로 정의될 수 있다.
- [0146] 암호화폐 믹싱 서비스는, 상술한 기술에 기초하여, 암호화폐를 보내는 지갑 주소와, 암호화폐를 수령하는 지갑 주소 간의 연결 관계를 숨길 수 있도록 하는 서비스일 수 있다.
- [0147] 블랙 마켓을 운영하는 주체는 소유하고 있는 지갑 주소들 및 지갑 주소들 간의 연결 관계가 숨김으로써 추적을 회피하려고 할 수 있다. 따라서, 블랙 마켓을 운영하는 주체는 믹싱 서비스를 이용할 수 있다.
- [0148] 따라서, 프로세서(110)는 믹싱 서비스에 이용되는 지갑들의 특성을 이용하여, 전체 트랜잭션 거래 내역에서 파악되는 지갑 주소들 중 믹싱 서비스에 이용되는 지갑들을 찾아낼 수 있다. 이를 통해, 전체 트랜잭션 거래 내역에서 파악되는 지갑 주소들 중 블랙 마켓 지갑 주소 및 상기 블랙 마켓 지갑 주소와 연결된 지갑 주소들을 선별하여 클러스터링할 수 있다.
- [0149] 도 3 내지 도 6에서 상술한 바에 의하여, 하나의 특정된 블랙 마켓 지갑 주소(910)가 프로세서(110)에 의하여 인식된 상황을 가정하자.
- [0150] 특정된 암호화폐 지갑 주소는 지속적으로 입출금을 수행할 수 있다. 도 4 및 도 6에서 제시된 바와 같이, 상기 암호화폐 지갑 주소로부터 생성된 파생 트랜잭션들을 연쇄적으로 추적할 경우, 상기 특정된 암호화폐 지갑 주소와 관련된 모든 암호화폐 지갑 주소들(920, 930 및 940)을 찾아낼 수 있다.
- [0151] 본 개시에 있어서 믹싱 서비스 지갑 주소(920)는 상술한 믹싱 서비스에 이용되는 지갑 주소들을 의미할 수 있다. 프로세서(110)는 메모리(120)로부터, 믹싱 서비스 지갑 주소들의 특징을 인식할 수 있다. 이에 기초하여, 프로세서(110)는 특정된 블랙 마켓 지갑 주소(910)와 관련된 모든 암호화폐 지갑 주소들 중 믹싱 서비스 지갑 주소(920)들을 인식할 수 있다.
- [0152] 일례로, 이러한 믹싱 서비스 지갑 주소(920)는 지갑 주소의 잔액(450) 또는 믹싱 서비스 지갑 주소(920)와 관련된 트랜잭션에 포함되는 암호화폐의 금액이 하기 [수학식 1]에 대응될 수 있다.

수학식 1

$$\text{잔액} = 2^{k*10^{(-n)}}$$

- [0153]
- [0155] 본 개시에 따른 암호화폐 지갑 주소 클러스터링 기법은 에스크로 서비스를 제공하는 블랙 마켓 지갑을 클러스터링 및 그룹화하려는 목적을 가지므로, 믹싱 서비스에 이용되는 지갑은 본 개시에 따른 방법에서 그룹화하려는 대상이 아닐 수 있다. 따라서, 프로세서(110)는 상기 [수학식 1]과 같은 잔액 정보를 갖는 지갑 주소들을 믹싱 서비스 지갑 주소(920)들로 분류하여, 이를 클러스터링 시 배제할 수 있다.
- [0156] 프로세서(110)는 전체 지갑 주소(910, 920, 930 및 940) 중에서 출금 지갑 주소(930)를 인식할 수 있다. 또한,

프로세서(110)는, 특정된 블랙 마켓 지갑 주소(910), 믹싱 서비스 지갑 주소(920) 및 출금 지갑 주소(930)를 제외한 나머지 지갑 주소가 블랙 마켓 지갑 주소에 해당된다고 판단할 수 있고, 이를 블랙 마켓 지갑 주소와 연결된 지갑 주소(940)로서 수집하여 클러스터링할 수 있다.

- [0158] 도 8은 본 개시의 몇몇 실시예에 따른 프로세서가 블랙 마켓 지갑 주소를 클러스터링 하는 것을 나타낸 순서도이다.
- [0159] 도 8을 참조하면, 프로세서(110)는 블랙 마켓 지갑 주소를 결정할 수 있다(S100).
- [0160] 본 개시에 있어서 블랙 마켓 지갑 주소는, 블랙 마켓을 운영하는 현실 주체가 에스크로 서비스를 제공하기 위해서 소유 및 이용하는 암호화폐 지갑/암호화폐 지갑의 주소를 의미할 수 있다.
- [0161] 본 개시의 몇몇 실시예에 따른 프로세서(110)는, 지갑 주소와 관련된 입금 트랜잭션과 상기 지갑 주소와 관련된 출금 트랜잭션 사이의 시간 간격, 상기 지갑 주소와 관련된 트랜잭션의 수, 상기 지갑 주소의 잔고에 대한 정보 또는 출금 트랜잭션들 간의 시간 간격 중 적어도 하나에 기초하여 상기 블랙 마켓 지갑 주소를 결정할 수 있다.
- [0162] 도 3에서 언급한 바와 같이, 일반적으로 블랙 마켓에서 이용하는 암호화폐 지갑(400)은 입금 트랜잭션과 출금 트랜잭션 간의 시간 간격이 짧거나, 일정 시간 간격으로 출금 트랜잭션이 수행된다는 특징이 있을 수 있다. 또한 일반적인 암호화폐 지갑들에 비해 짧은 기간 동안 많은 트랜잭션 수(420)를 갖는다는 특징이 있을 수 있다. 이에 더하여, 입금된 전체 금액(430)과 출금된 전체 금액(440)이 동일하고, 따라서 잔액(450)이 0이라는 특징이 있을 수 있다. 또한 일정 기간 동안 사용된 이후에는 더 이상 사용되지 않는다는 특징을 가질 수 있다.
- [0163] 프로세서(110)는 상술한 특징들을 이용하여 특정 암호화폐 지갑 주소가 블랙 마켓에 의하여 운영되는지 여부를 판단할 수 있다. 가령, 프로세서(110)는, 임의의 암호화폐 지갑 주소가 블랙 마켓 지갑 주소의 특징들 중 기 설정된 비율(예를 들면, 절반) 이상의 특징을 가지면 이를 블랙 마켓 지갑 주소로 결정하도록 할 수 있다.
- [0164] 본 개시의 블랙 마켓 지갑 주소는 도 3의 지갑 주소(410), 도 4의 입금 트랜잭션(531) 및 출금 트랜잭션(532)에 포함된 지갑 주소들 중 어느 하나, 도 5의 웹 페이지에 포함된 암호화폐 지갑 주소(610) 중 적어도 하나로서 수집 및 결정될 수 있다.
- [0165] 상술한 내용은 블랙 마켓 지갑 주소가 수집 및 결정되는 방법의 일례에 불과하며, 블랙 마켓 지갑 주소의 수집 및 결정 방법은 이에 한정되지 않는다.
- [0166] 이러한 지갑 주소들은 도 7에서 블랙 마켓 지갑 주소(910)로 도식화될 수 있다.
- [0167] 프로세서(110)는 블랙 마켓 지갑 주소에 대해 수행된 하나 이상의 트랜잭션을 인식할 수 있다(S200).
- [0168] 프로세서(110)는 단계(S100)에서 결정된 블랙 마켓 지갑 주소의 트랜잭션 내역을 검토함으로써, 결정된 블랙 마켓 지갑 주소에 대해 수행된 하나 이상의 트랜잭션을 인식할 수 있다.
- [0169] 일례로, 블랙 마켓 지갑 주소의 트랜잭션 내역은 도 4에 도시된 트랜잭션 내역(500)일 수 있다. 프로세서(110)는 트랜잭션 내역(500)에 포함된 개별 트랜잭션 입금 트랜잭션(531) 및 출금 트랜잭션(532)들을 인식할 수 있다. 다만 이는 블랙 마켓 지갑 주소에 대해 수행된 하나 이상의 트랜잭션들을 인식하기 위한 방법의 예시에 불과하다. 따라서, 블랙 마켓 지갑 주소에 대해 수행된 하나 이상의 트랜잭션들을 인식하기 위한 방법은 이에 한정되지 않는다.
- [0170] 프로세서(110)는 하나 이상의 트랜잭션에 기초하여, 블랙 마켓 지갑 주소와 연결된 지갑 주소들을 수집할 수 있다(S300).
- [0171] 본 개시에 있어서, 연결된 지갑 주소들은, 상기 결정된 블랙 마켓 지갑 주소로부터 암호화폐를 입금받거나, 결정된 블랙 마켓 지갑 주소에 대해 암호화폐를 송금하는 등의 행위를 수행한 지갑 주소들을 의미할 수 있다.
- [0172] 이러한 연결된 지갑 주소들은 상기 결정된 블랙 마켓 지갑 주소와 관련된 모든 트랜잭션들을 추적함으로써 수집될 수 있다.
- [0173] 위에서 언급한 도면들을 예시로 들면, 본 개시에 따른 연결된 지갑 주소들은 도 4의 입금 트랜잭션(531) 및 출금 트랜잭션(532)에 포함된 지갑 주소들을 포함할 수 있다.
- [0174] 프로세서(110)는 블랙 마켓 지갑 주소 및 수집된 지갑 주소들을 하나의 그룹으로 클러스터링할 수 있다(S400).

- [0175] 본 개시에 있어서 클러스터링은, 블랙 마켓 운영주체가 소유 및 사용하는 암호화폐 지갑 주소들을 하나의 그룹에 포함시키는 것을 의미할 수 있다.
- [0176] 프로세서(110)는 블랙 마켓 지갑 주소와 단계(S300)를 통해 수집된 상기 연결된 지갑 주소들을 하나의 그룹에 포함시킴으로써, 클러스터링을 수행할 수 있다.
- [0177] 이에 따라, 블록체인 기술 및 암호화폐에 기반하여 블랙 마켓 상에서 이루어지는 불법적인 거래들을 추적할 수 있다. 또한, 블랙 마켓에서 이용하는 하나의 지갑 주소를 아는 것 만으로도 연관된 다수의 지갑 주소를 한 번에 파악할 수 있다. 불법 거래 및 이와 관련된 암호화폐 지갑들의 추적 및 제재가 용이해질 수 있다.
- [0178] 프로세서(110)는 하나의 그룹으로 클러스터링된 지갑 주소들의 거래 종료시점을 인식할 수 있다(S500).
- [0179] 일반적으로 블랙 마켓 운영 주체들은, 생성된 암호화폐 지갑 주소를 일정 기간 동안만 사용하고, 더 이상 사용하지 않는 것으로 알려져 있다. 이를 통해 운영 주체들은 수사 기관 및 사법 기관 등의 추적을 회피할 수 있다.
- [0180] 이에 대응하여, 프로세서(110)는 클러스터링된 지갑 주소들 중 더 이상 사용되지 않는 지갑들을 분별해내기 위해, 클러스터링된 지갑 주소들 각각의 거래 종료 시점을 인식할 수 있다.
- [0181] 프로세서(110)는 거래 종료 시점이 기 설정된 기간 이상인 적어도 하나의 지갑 주소를 그룹에서 제외할 수 있다(S600).
- [0182] 일정 기간 이상 거래가 진행되지 않은 지갑 주소들을 그룹에 지속적으로 보관할 경우, 추가적인 추적 및 클러스터링 시 프로세서(110)의 연산량이 불필요하게 늘어날 수 있다.
- [0183] 따라서, 주기적으로 거래가 종료된(더 이상 블랙 마켓에 의해 운용되지 않는) 지갑 주소들을 선별해내고, 이를 그룹에서 제외함으로써, 본 개시에 따른 블랙 마켓 지갑 주소 추적을 효율적으로 수행할 수 있다.
- [0185] 도 9는 본 개시의 몇몇 실시예에 따른 프로세서가 제 1 블랙 마켓 지갑 주소를 결정하는 것을 나타낸 순서도이다.
- [0186] 프로세서(110)는 웹 크롤러를 이용해 수집된 지갑 주소와, 하나 이상의 다른 지갑 주소가 결합되어 생성된 출금 트랜잭션을 인식할 수 있다(S110).
- [0187] 도 5에서 전술한 바와 같이, 본 개시에 있어서 웹 크롤러는 인터넷 상에 있는 자료를 가져와 데이터 분석하기 쉬운 형태로 가공하는 작업을 수행하는 모듈을 의미할 수 있다.
- [0188] 예를 들어, 본 개시에 따른 프로세서(110)는 상기 웹 크롤러를 이용하여 블랙 마켓 지갑 주소를 수집할 수 있다.
- [0189] 웹 크롤러를 이용해 블랙 마켓 지갑 주소를 수집하면, 자동적으로 수많은 웹 페이지에 대하여 블랙 마켓 지갑 주소를 수집해낼 수 있다. 따라서, 동시에 수집할 수 있는 블랙 마켓 지갑 주소 및 그와 연결된 지갑 주소들의 수가 증가할 수 있다. 따라서, 블랙 마켓에 의하여 수행되는 불법 거래에 대한 추적 및 제재가 용이해질 수 있다.
- [0190] 일반적인 블록체인 및 암호화폐 지갑과 관련된 클라이언트 프로그램들은 복수의 주소가 결합하여 하나의 트랜잭션을 생성할 수 있도록 지원할 수 있다. 그러나, 이러한 클라이언트들은 일반적으로 복수의 사용자들이 하나의 트랜잭션을 생성하는 것을 지원하지 않을 수 있다. 따라서, 복수의 지갑 주소로부터 출금이 이루어지는 트랜잭션의 경우라도 해당 트랜잭션은 한 명의 사용자에 의해 생성된 것이라고 볼 수 있다. 이 경우, 출금이 이루어진 복수의 지갑 주소는 한 명의 사용자와 연관된다고 볼 수 있다.
- [0191] 프로세서(110)는 출금 트랜잭션에 포함된, 웹 크롤러를 이용하여 수집된 지갑 주소 및 하나 이상의 다른 지갑 주소 각각을 블랙 마켓 지갑 주소로 결정할 수 있다(S120).
- [0192] 상술한 특징에 더하여, 블랙 마켓 지갑 주소들은 구매자와 판매자에 대한 입금 및 출금 외에는 상호 간에만 입출금을 수행한다는 특징이 있다.
- [0193] 이러한 특징에 기초하면, 블랙 마켓 지갑 주소를 포함하는 복수의 지갑 주소로부터 하나의 암호화폐 지갑 주소로 암호화폐의 전송이 이루어진 경우, 출금이 이루어진 복수의 지갑 주소들이 블랙 마켓 운영 주체에 의하여 운영되는 지갑 주소라고 판단할 수 있다.

- [0194] 따라서, 프로세서(110)는 암호화폐가 출금되는 복수의 지갑 주소들을, 클러스터링 작업을 수행하기 위한 시발점이 되는 블랙 마켓 지갑 주소로 결정할 수 있다. 이 경우, 프로세서(110)는 복수의 지갑 주소들 각각에 대하여 본 개시에 따른 클러스터링 기법을 적용하여, 동시에 더 많은 블랙 마켓 지갑 주소들을 발견해낼 수 있다.
- [0195] 이러한 특징을 이용하면, 블랙 마켓 지갑 주소를 단 하나만 특정하더라도 다수의 블랙 마켓 지갑 주소들을 한꺼번에 발견해낼 수 있다. 따라서 블랙 마켓에서 이루어지는 불법 거래 행위의 추적이 용이할 수 있다.
- [0196] 이는 사용자에게 대해서 복수의 지갑 주소들을 클러스터링 하기 위한 방법의 하나의 예시일 뿐이므로, 클러스터링 하기 위한 방법은 이에 한정되지 않는다.
- [0198] 도 10은 본 개시의 몇몇 실시예에 따른 프로세서가 블랙 마켓 지갑 주소와 연결된 지갑 주소들을 수집하는 것을 나타낸 순서도이다.
- [0199] 도 10을 참조하면, 프로세서(110)는 하나 이상의 트랜잭션으로부터 파생된 하나 이상의 파생 트랜잭션을 인식할 수 있다(S310).
- [0200] 본 개시에 있어 파생 트랜잭션은, 암호화폐 지갑 주소로 입금된 이전 트랜잭션에 기초하여 새로이 생성된 트랜잭션을 의미할 수 있다.
- [0201] 도 6을 다시 참조하면, 제 2 트랜잭션(710b)을 통해 지갑 주소(411)에 0.06131465 BTC가 입금된 것을 확인할 수 있다. 그리고, 당해 지갑 주소(411)는 이미 0.30815704 BTC를 추가적으로 보유하고 있음을 파생 트랜잭션(800)의 화살표 좌측을 통해 알 수 있다.
- [0202] 지갑 주소(411)와 관련된 주체는, 지갑 주소(411)가 이미 보유하고 있었던 금액과, 제 2 트랜잭션(710b)을 통해 입금된 금액을 결합하여 새로운 트랜잭션을 생성할 수 있으며, 파생 트랜잭션(800)은 그 일례이다.
- [0203] 상술한 바와 같이, 블랙 마켓 지갑 주소들은 서로 간에만 암호화폐를 전송하는 특징을 가지고 있다. 따라서, 파생 트랜잭션에서 입출금이 수행되는 모든 지갑 주소들은 블랙 마켓 지갑 주소와 관련된 주체의 소유일 가능성이 높을 수 있다. 따라서, 프로세서(110)들은 파생 트랜잭션(800)에 포함된 모든 암호화폐 지갑 주소들을 하나의 주체에 대하여 클러스터링 할 수 있다.
- [0204] 다시 도 10을 참조하면, 프로세서(110)는 파생 트랜잭션 각각에 포함된 하나 이상의 지갑 주소를 연결된 지갑 주소들로 수집할 수 있다(S320).
- [0205] 블랙 마켓 지갑 주소들은 구매자와 판매자에 대한 입금 및 출금 외에는 상호 간에만 입출금을 수행한다.
- [0206] 이러한 특징에 기초하면, 블랙 마켓 지갑 주소를 포함하는 복수의 지갑 주소로부터 하나의 암호화폐 지갑 주소로 암호화폐의 전송이 이루어진 경우, 출금이 이루어진 복수의 지갑 주소들이 블랙 마켓 지갑 주소와 연결된 지갑 주소라고 판단할 수 있다.
- [0207] 파생 트랜잭션(800)의 경우에도, 파생 트랜잭션(800)에 포함된 암호화폐 지갑 주소 중 적어도 하나가 블랙 마켓 지갑 주소 또는 이와 연결된 지갑 주소라면, 파생 트랜잭션(800)에 포함된 나머지 지갑 주소들도 블랙 마켓 지갑 주소와 연결된 지갑 주소일 수 있다. 따라서, 프로세서(110)는 파생 트랜잭션(800)에 포함된 모든 지갑 주소들을 상기 연결된 지갑 주소로 결정하고, 하나의 그룹으로 클러스터링 할 수 있다.
- [0208] 이러한 특징을 이용하면, 블랙 마켓 지갑 주소를 단 하나만 특정하더라도 다수의 블랙 마켓 지갑 주소들을 한꺼번에 발견해낼 수 있다. 따라서 블랙 마켓에서 이루어지는 불법 거래 행위의 추적이 용이할 수 있다.
- [0209] 이는 사용자에게 대해서 복수의 지갑 주소들을 클러스터링 하기 위한 방법의 하나의 예시일 뿐이므로, 클러스터링 하기 위한 방법은 이에 한정되지 않는다.
- [0211] 도 11은 본 개시의 몇몇 실시예에 따른 프로세서가 블랙 마켓 지갑 주소와 연결된 지갑 주소들을 수집하는 것을 나타낸 순서도이다.
- [0212] 도 11을 참조하면, 프로세서(110)는 파생 트랜잭션에 포함된 하나 이상의 지갑 주소 각각이, 하나 이상의 다른 지갑 주소와 결합되어 생성된 출금 트랜잭션을 인식할 수 있다(S330).
- [0213] 일반적인 블록체인 및 암호화폐 지갑과 관련된 클라이언트 프로그램들은 복수의 주소가 결합하여 하나의 트랜잭

션을 생성할 수 있도록 지원한다. 그러나, 이러한 클라이언트들은 일반적으로 복수의 사용자들이 하나의 트랜잭션을 생성하는 것을 지원하지 않는다(출원시점 기준). 따라서, 복수의 지갑 주소로부터 출금이 이루어지는 트랜잭션의 경우라도 해당 트랜잭션은 한 명의 사용자에 의해 생성된 것이라고 볼 수 있다. 따라서, 이 경우, 출금이 이루어진 복수의 지갑 주소는 한 명의 사용자와 연관된다고 볼 수 있다.

- [0214] 도 4를 다시 참조하면, 출금 트랜잭션(532)은 화살표 좌측의 복수의 지갑 주소들에 의해 출금이 수행되었다. 그러나 상술한 바와 같이, 암호화폐 클라이언트의 특성 상, 당해 복수의 지갑 주소들은 모두 동일한 블록체인 또는 암호화폐 사용 주체의 소유라고 볼 수 있다.
- [0215] 이러한 특성에 기초하여 프로세서(110)는 복수의 지갑 주소를 블랙 마켓 지갑 주소와 연결된 지갑 주소들로 결정할 수 있다. 이에, 프로세서(110)는 상기 블랙 마켓 지갑 주소 및 연결된 지갑 주소들을 하나의 암호화폐 사용 주체에 대하여 클러스터링 할 수 있다. 즉, 출금 트랜잭션(532)과 같이, 하나의 트랜잭션 내에서 복수의 지갑 주소들에 의해 출금이 수행된 경우, 상기 복수의 지갑 주소들은 한 명의 사용자에 대해 클러스터링 될 수 있을 것이다.
- [0216] 이는 사용자에 대해서 복수의 지갑 주소들을 클러스터링 하기 위한 방법의 하나의 예시일 뿐이므로, 클러스터링 하기 위한 방법은 이에 한정되지 않는다.
- [0217] 도 11을 다시 참조하면, 프로세서(110)는, 파생 트랜잭션에 포함된 하나 이상의 지갑 주소 및 하나 이상의 다른 지갑 주소 각각을 연결된 지갑 주소들로 수집할 수 있다(S340).
- [0218] 본 개시에 있어서, 연결된 지갑 주소들은, 상기 결정된 블랙 마켓 지갑 주소로부터 암호화폐를 입금받거나, 결정된 블랙 마켓 지갑 주소에 대해 암호화폐를 송금하는 등의 행위를 수행한 지갑 주소들을 의미할 수 있다.
- [0219] 이러한 연결된 지갑 주소들은 상기 결정된 블랙 마켓 지갑 주소와 관련된 모든 트랜잭션들을 추적함으로써 수집될 수 있다.
- [0220] 위에서 언급한 도면들을 예시로 들면, 본 개시에 따른 연결된 지갑 주소들은 도 4의 입금 트랜잭션(531) 및 출금 트랜잭션(532)에 포함된 지갑 주소들을 포함할 수 있다.
- [0221] 상술한 바에 의하여, 블랙 마켓 지갑 주소를 단 하나만 특정하더라도 다수의 블랙 마켓 지갑 주소들을 한꺼번에 발견해낼 수 있다. 따라서 블랙 마켓에서 이루어지는 불법 거래 행위의 추적이 용이할 수 있다.
- [0223] 도 12는 본 개시의 몇몇 실시예들이 구현될 수 있는 예시적인 컴퓨팅 환경에 대한 간략하고 일반적인 개략도를 도시한다.
- [0224] 도 12에서 도시되는 컴퓨터(1102)는, 컴퓨팅 장치(100) 및 블록체인 네트워크(200)에 포함된 컴퓨팅 장치 중 적어도 하나에 대응될 수 있다.
- [0225] 본 개시내용이 일반적으로 하나 이상의 컴퓨터 상에서 실행될 수 있는 컴퓨터 실행가능 명령어와 관련하여 기술되었지만, 당업자라면 본 개시내용 기타 프로그램 모듈들과 결합되어 및/또는 하드웨어와 소프트웨어의 조합으로서 구현될 수 있다는 것을 잘 알 것이다.
- [0226] 일반적으로, 본 명세서에서의 모듈은 특정의 태스크를 수행하거나 특정의 추상 데이터 유형을 구현하는 루틴, 프로시저, 프로그램, 컴포넌트, 데이터 구조, 기타 등등을 포함한다. 또한, 당업자라면 본 개시의 방법이 단일-프로세서 또는 멀티프로세서 컴퓨터 시스템, 미니컴퓨터, 메인프레임 컴퓨터는 물론 퍼스널 컴퓨터, 핸드헬드 컴퓨팅 장치, 마이크로프로세서-기반 또는 프로그램가능 가전 제품, 기타 등등(이들 각각은 하나 이상의 연관된 장치와 연결되어 동작할 수 있음)을 비롯한 다른 컴퓨터 시스템 구성으로 실시될 수 있다는 것을 잘 알 것이다.
- [0227] 본 개시의 설명된 실시예들은 또한 어떤 태스크들이 통신 네트워크를 통해 연결되어 있는 원격 처리 장치들에 의해 수행되는 분산 컴퓨팅 환경에서 실시될 수 있다. 분산 컴퓨팅 환경에서, 프로그램 모듈은 로컬 및 원격 메모리 저장 장치 둘다에 위치할 수 있다.
- [0228] 컴퓨터는 통상적으로 다양한 컴퓨터 판독가능 매체를 포함한다. 컴퓨터에 의해 액세스 가능한 매체로서, 휘발성 및 비휘발성 매체, 일시적(transitory) 및 비일시적(non-transitory) 매체, 이동식 및 비-이동식 매체를 포함한다. 제한이 아닌 예로서, 컴퓨터 판독가능 매체는 컴퓨터 판독가능 저장 매체 및 컴퓨터 판독가능 전송 매체를 포함할 수 있다.

- [0229] 컴퓨터 판독가능 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보를 저장하는 임의의 방법 또는 기술로 구현되는 휘발성 및 비휘발성 매체, 일시적 및 비-일시적 매체, 이동식 및 비이동식 매체를 포함한다. 컴퓨터 판독가능 저장 매체는 RAM, ROM, EEPROM, 플래시 메모리 또는 기타 메모리 기술, CD-ROM, DVD(digital video disk) 또는 기타 광 디스크 저장 장치, 자기 카세트, 자기 테이프, 자기 디스크 저장 장치 또는 기타 자기 저장 장치, 또는 컴퓨터에 의해 액세스될 수 있고 원하는 정보를 저장하는데 사용될 수 있는 임의의 기타 매체를 포함하지만, 이에 한정되지 않는다.
- [0230] 컴퓨터 판독가능 전송 매체는 통상적으로 반송파(carrier wave) 또는 기타 전송 메커니즘(transport mechanism)과 같은 피변조 데이터 신호(modulated data signal)에 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터들을 구현하고 모든 정보 전달 매체를 포함한다. 피변조 데이터 신호라는 용어는 신호 내에 정보를 인코딩하도록 그 신호의 특성들 중 하나 이상을 설정 또는 변경시킨 신호를 의미한다. 제한이 아닌 예로서, 컴퓨터 판독가능 전송 매체는 유선 네트워크 또는 직접 배선 접속(direct-wired connection)과 같은 유선 매체, 그리고 음향, RF, 적외선, 기타 무선 매체와 같은 무선 매체를 포함한다. 상술된 매체들 중 임의의 것의 조합도 역시 컴퓨터 판독가능 전송 매체의 범위 안에 포함되는 것으로 한다.
- [0231] 컴퓨터(1102)를 포함하는 본 개시의 여러가지 측면들을 구현하는 예시적인 환경(1100)이 나타내어져 있으며, 컴퓨터(1102)는 처리 장치(1104), 시스템 메모리(1106) 및 시스템 버스(1108)를 포함한다. 시스템 버스(1108)는 시스템 메모리(1106)(이에 한정되지 않음)를 비롯한 시스템 컴포넌트들을 처리 장치(1104)에 연결시킨다. 처리 장치(1104)는 다양한 상용 프로세서들 중 임의의 프로세서일 수 있다. 듀얼 프로세서 및 기타 멀티프로세서 아키텍처도 역시 처리 장치(1104)로서 이용될 수 있다.
- [0232] 시스템 버스(1108)는 메모리 버스, 주변장치 버스, 및 다양한 상용 버스 아키텍처 중 임의의 것을 사용하는 로컬 버스에 추가적으로 상호 연결될 수 있는 몇가지 유형의 버스 구조 중 임의의 것일 수 있다. 시스템 메모리(1106)는 판독 전용 메모리(ROM)(1110) 및 랜덤 액세스 메모리(RAM)(1112)를 포함한다. 기본 입/출력 시스템(BIOS)은 ROM, EPROM, EEPROM 등의 비휘발성 메모리(1110)에 저장되며, 이 BIOS는 시동 중과 같은 때에 컴퓨터(1102) 내의 구성요소들 간에 정보를 전송하는 일을 돕는 기본적인 루틴을 포함한다. RAM(1112)은 또한 데이터를 캐싱하기 위한 정적 RAM 등의 고속 RAM을 포함할 수 있다.
- [0233] 컴퓨터(1102)는 또한 내장형 하드 디스크 드라이브(HDD)(1114)(예를 들어, EIDE, SATA)—이 내장형 하드 디스크 드라이브(1114)는 또한 적당한 새시(도시 생략) 내에서 외장형 용도로 구성될 수 있음—, 자기 플로피 디스크 드라이브(FDD)(1116)(예를 들어, 이동식 디스켓(1118)으로부터 판독을 하거나 그에 기록을 하기 위한 것임), 및 광 디스크 드라이브(1120)(예를 들어, CD-ROM 디스크(1122)를 판독하거나 DVD 등의 기타 고용량 광 매체로부터 판독을 하거나 그에 기록을 하기 위한 것임)를 포함한다. 하드 디스크 드라이브(1114), 자기 디스크 드라이브(1116) 및 광 디스크 드라이브(1120)는 각각 하드 디스크 드라이브 인터페이스(1124), 자기 디스크 드라이브 인터페이스(1126) 및 광 드라이브 인터페이스(1128)에 의해 시스템 버스(1108)에 연결될 수 있다. 외장형 드라이브 구현을 위한 인터페이스(1124)는 예를 들어, USB(Universal Serial Bus) 및 IEEE 1394 인터페이스 기술 중 적어도 하나 또는 그 둘다를 포함한다.
- [0234] 이들 드라이브 및 그와 연관된 컴퓨터 판독가능 매체는 데이터, 데이터 구조, 컴퓨터 실행가능 명령어, 기타 등등의 비휘발성 저장을 제공한다. 컴퓨터(1102)의 경우, 드라이브 및 매체는 임의의 데이터를 적당한 디지털 형식으로 저장하는 것에 대응한다. 상기에서의 컴퓨터 판독가능 저장 매체에 대한 설명이 HDD, 이동식 자기 디스크, 및 CD 또는 DVD 등의 이동식 광 매체를 언급하고 있지만, 당업자라면 zip 드라이브(zip drive), 자기 카세트, 플래시 메모리 카드, 카트리지, 기타 등등의 컴퓨터에 의해 판독가능한 다른 유형의 저장 매체도 역시 예시적인 운영 환경에서 사용될 수 있으며 또 임의의 이러한 매체가 본 개시의 방법들을 수행하기 위한 컴퓨터 실행가능 명령어를 포함할 수 있다는 것을 잘 알 것이다.
- [0235] 운영 체제(1130), 하나 이상의 애플리케이션 프로그램(1132), 기타 프로그램 모듈(1134) 및 프로그램 데이터(1136)를 비롯한 다수의 프로그램 모듈이 드라이브 및 RAM(1112)에 저장될 수 있다. 운영 체제, 애플리케이션, 모듈 및/또는 데이터의 전부 또는 그 일부분이 또한 RAM(1112)에 캐싱될 수 있다. 본 개시가 여러가지 상업적으로 이용가능한 운영 체제 또는 운영 체제들의 조합에서 구현될 수 있다는 것을 잘 알 것이다.
- [0236] 사용자는 하나 이상의 유선/무선 입력 장치, 예를 들어, 키보드(1138) 및 마우스(1140) 등의 포인팅 장치를 통해 컴퓨터(1102)에 명령 및 정보를 입력할 수 있다. 기타 입력 장치(도시 생략)로는 마이크, IR 리모콘, 조이스틱, 게임 패드, 스타일러스 펜, 터치 스크린, 기타 등등이 있을 수 있다. 이들 및 기타 입력 장치가 종종 시스템 버스(1108)에 연결되어 있는 입력 장치 인터페이스(1142)를 통해 처리 장치(1104)에 연결되지만, 병렬 포트,

IEEE 1394 직렬 포트, 게임 포트, USB 포트, IR 인터페이스, 기타 등등의 기타 인터페이스에 의해 연결될 수 있다.

[0237] 모니터(1144) 또는 다른 유형의 디스플레이 장치도 역시 비디오 어댑터(1146) 등의 인터페이스를 통해 시스템 버스(1108)에 연결된다. 모니터(1144)에 부가하여, 컴퓨터는 일반적으로 스피커, 프린터, 기타 등등의 기타 주변 출력 장치(도시 생략)를 포함한다.

[0238] 컴퓨터(1102)는 유선 및/또는 무선 통신을 통한 원격 컴퓨터(들)(1148) 등의 하나 이상의 원격 컴퓨터로의 논리적 연결을 사용하여 네트워크화된 환경에서 동작할 수 있다. 원격 컴퓨터(들)(1148)는 워크스테이션, 서버 컴퓨터, 라우터, 퍼스널 컴퓨터, 휴대용 컴퓨터, 마이크로프로세서-기반 오락 기기, 피어 장치 또는 기타 통상의 네트워크 노드일 수 있으며, 일반적으로 컴퓨터(1102)에 대해 기술된 구성요소들 중 다수 또는 그 전부를 포함하지만, 간략함을 위해, 메모리 저장 장치(1150)만이 도시되어 있다. 도시되어 있는 논리적 연결은 근거리 통신망(LAN)(1152) 및/또는 더 큰 네트워크, 예를 들어, 원거리 통신망(WAN)(1154)에의 유선/무선 연결을 포함한다. 이러한 LAN 및 WAN 네트워킹 환경은 사무실 및 회사에서 일반적인 것이며, 인트라넷 등의 전사적 컴퓨터 네트워크(enterprise-wide computer network)를 용이하게 해주며, 이들 모두는 전세계 컴퓨터 네트워크, 예를 들어, 인터넷에 연결될 수 있다.

[0239] LAN 네트워킹 환경에서 사용될 때, 컴퓨터(1102)는 유선 및/또는 무선 통신 네트워크 인터페이스 또는 어댑터(1156)를 통해 로컬 네트워크(1152)에 연결된다. 어댑터(1156)는 LAN(1152)에의 유선 또는 무선 통신을 용이하게 해줄 수 있으며, 이 LAN(1152)은 또한 무선 어댑터(1156)와 통신하기 위해 그에 설치되어 있는 무선 액세스 포인트를 포함하고 있다. WAN 네트워킹 환경에서 사용될 때, 컴퓨터(1102)는 모뎀(1158)을 포함할 수 있거나, WAN(1154) 상의 통신 서버에 연결되거나, 또는 인터넷을 통하는 등, WAN(1154)을 통해 통신을 설정하는 기타 수단을 갖는다. 내장형 또는 외장형 및 유선 또는 무선 장치일 수 있는 모뎀(1158)은 직렬 포트 인터페이스(1142)를 통해 시스템 버스(1108)에 연결된다. 네트워크화된 환경에서, 컴퓨터(1102)에 대해 설명된 프로그램 모듈들 또는 그의 일부분이 원격 메모리/저장 장치(1150)에 저장될 수 있다. 도시된 네트워크 연결이 예시적인 것이며 컴퓨터들 사이에 통신 링크를 설정하는 기타 수단이 사용될 수 있다는 것을 잘 알 것이다.

[0240] 컴퓨터(1102)는 무선 통신으로 배치되어 동작하는 임의의 무선 장치 또는 개체, 예를 들어, 프린터, 스캐너, 데스크톱 및/또는 휴대용 컴퓨터, PDA(portable data assistant), 통신 위성, 무선 검출가능 태그와 연관된 임의의 장비 또는 장소, 및 전화와 통신을 하는 동작을 한다. 이것은 적어도 Wi-Fi 및 블루투스 무선 기술을 포함한다. 따라서, 통신은 종래의 네트워크에서와 같이 미리 정의된 구조이거나 단순히 적어도 2개의 장치 사이의 애드혹 통신(ad hoc communication)일 수 있다.

[0241] Wi-Fi(Wireless Fidelity)는 유선 없이도 인터넷 등으로의 연결을 가능하게 해준다. Wi-Fi는 이러한 장치, 예를 들어, 컴퓨터가 실내에서 및 실외에서, 즉 기지국의 통화권 내의 아무 곳에서나 데이터를 전송 및 수신할 수 있게 해주는 셀 전화와 같은 무선 기술이다. Wi-Fi 네트워크는 안전하고 신뢰성 있으며 고속인 무선 연결을 제공하기 위해 IEEE 802.11(a,b,g, 기타)이라고 하는 무선 기술을 사용한다. 컴퓨터를 서로에, 인터넷에 및 유선 네트워크(IEEE 802.3 또는 이더넷을 사용함)에 연결시키기 위해 Wi-Fi가 사용될 수 있다. Wi-Fi 네트워크는 비인가 2.4 및 5 GHz 무선 대역에서, 예를 들어, 11Mbps(802.11a) 또는 54 Mbps(802.11b) 데이터 레이트로 동작하거나, 양 대역(듀얼 대역)을 포함하는 제품에서 동작할 수 있다.

[0242] 본 개시의 기술 분야에서 통상의 지식을 가진 자는 여기에 개시된 실시예들과 관련하여 설명된 다양한 예시적인 논리 블록들, 모듈들, 프로세서들, 수단들, 회로들 및 알고리즘 단계들이 전자 하드웨어, (편의를 위해, 여기에서 "소프트웨어"로 지칭되는) 다양한 형태들의 프로그램 또는 설계 코드 또는 이들 모두의 결합에 의해 구현될 수 있다는 것을 이해할 것이다. 하드웨어 및 소프트웨어의 이러한 상호 호환성을 명확하게 설명하기 위해, 다양한 예시적인 컴포넌트들, 블록들, 모듈들, 회로들 및 단계들이 이들의 기능과 관련하여 위에서 일반적으로 설명되었다. 이러한 기능이 하드웨어 또는 소프트웨어로서 구현되는지 여부는 특정한 애플리케이션 및 전체 시스템에 대하여 부과되는 설계 제약들에 따라 좌우된다. 본 개시의 기술 분야에서 통상의 지식을 가진 자는 각각의 특정한 애플리케이션에 대하여 다양한 방식으로 설명된 기능을 구현할 수 있으나, 이러한 구현 결정들은 본 개시의 범위를 벗어나는 것으로 해석되어서는 안 될 것이다.

[0243] 여기서 제시된 다양한 실시예들은 방법, 장치, 또는 표준 프로그래밍 및/또는 엔지니어링 기술을 사용한 제조물품(article)으로 구현될 수 있다. 용어 "제조물품"은 임의의 컴퓨터-판독가능 장치로부터 액세스 가능한 컴퓨터 프로그램, 캐리어, 또는 매체(media)를 포함한다. 예를 들어, 컴퓨터-판독가능 저장 매체는 자기 저장 장치(예를 들면, 하드 디스크, 플로피 디스크, 자기 스트림, 등), 광학 디스크(예를 들면, CD, DVD, 등), 스마트

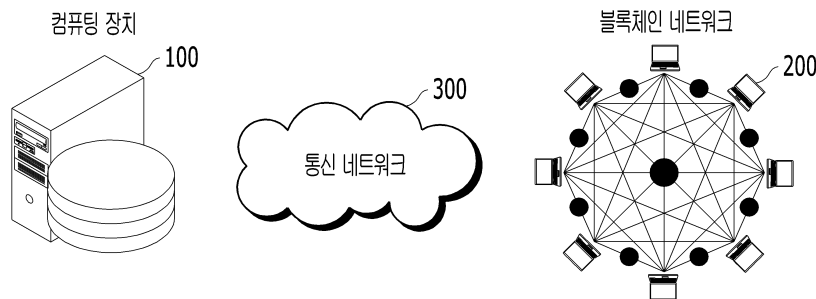
카드, 및 플래쉬 메모리 장치(예를 들면, EEPROM, 카드, 스틱, 키 드라이브, 등)를 포함하지만, 이들로 제한되는 것은 아니다. 용어 "기계-판독가능 매체"는 명령(들) 및/또는 데이터를 저장, 보유, 및/또는 전달할 수 있는 무선 채널 및 다양한 다른 매체를 포함하지만, 이들로 제한되는 것은 아니다.

[0244] 제시된 프로세스들에 있는 단계들의 특정한 순서 또는 계층 구조는 예시적인 접근들의 일례임을 이해하도록 한다. 실제 우선순위들에 기반하여, 본 개시의 범위 내에서 프로세스들에 있는 단계들의 특정한 순서 또는 계층 구조가 재배열될 수 있다는 것을 이해하도록 한다. 첨부된 방법 청구항들은 샘플 순서로 다양한 단계들의 엘리먼트들을 제공하지만 제시된 특정한 순서 또는 계층 구조에 한정되는 것을 의미하지는 않는다.

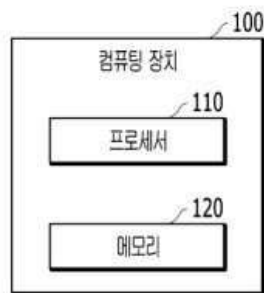
[0246] 제시된 실시예들에 대한 설명은 임의의 본 개시의 기술 분야에서 통상의 지식을 가진 자가 본 개시를 이용하거나 또는 실시할 수 있도록 제공된다. 이러한 실시예들에 대한 다양한 변형들은 본 개시의 기술 분야에서 통상의 지식을 가진 자에게 명백할 것이며, 여기에 정의된 일반적인 원리들은 본 개시의 범위를 벗어남이 없이 다른 실시예들에 적용될 수 있다. 그리하여, 본 개시는 여기에 제시된 실시예들로 한정되는 것이 아니라, 여기에 제시된 원리들 및 신규한 특징들과 일관되는 최광의의 범위에서 해석되어야 할 것이다.

도면

도면1



도면2



도면3

400



Address 39rEZVYa1ecqA5q4eg4gHXF7G... 410

Format BASE58 (P2SH)

Transactions 36 420

Total Received 0.30830651 BTC 430

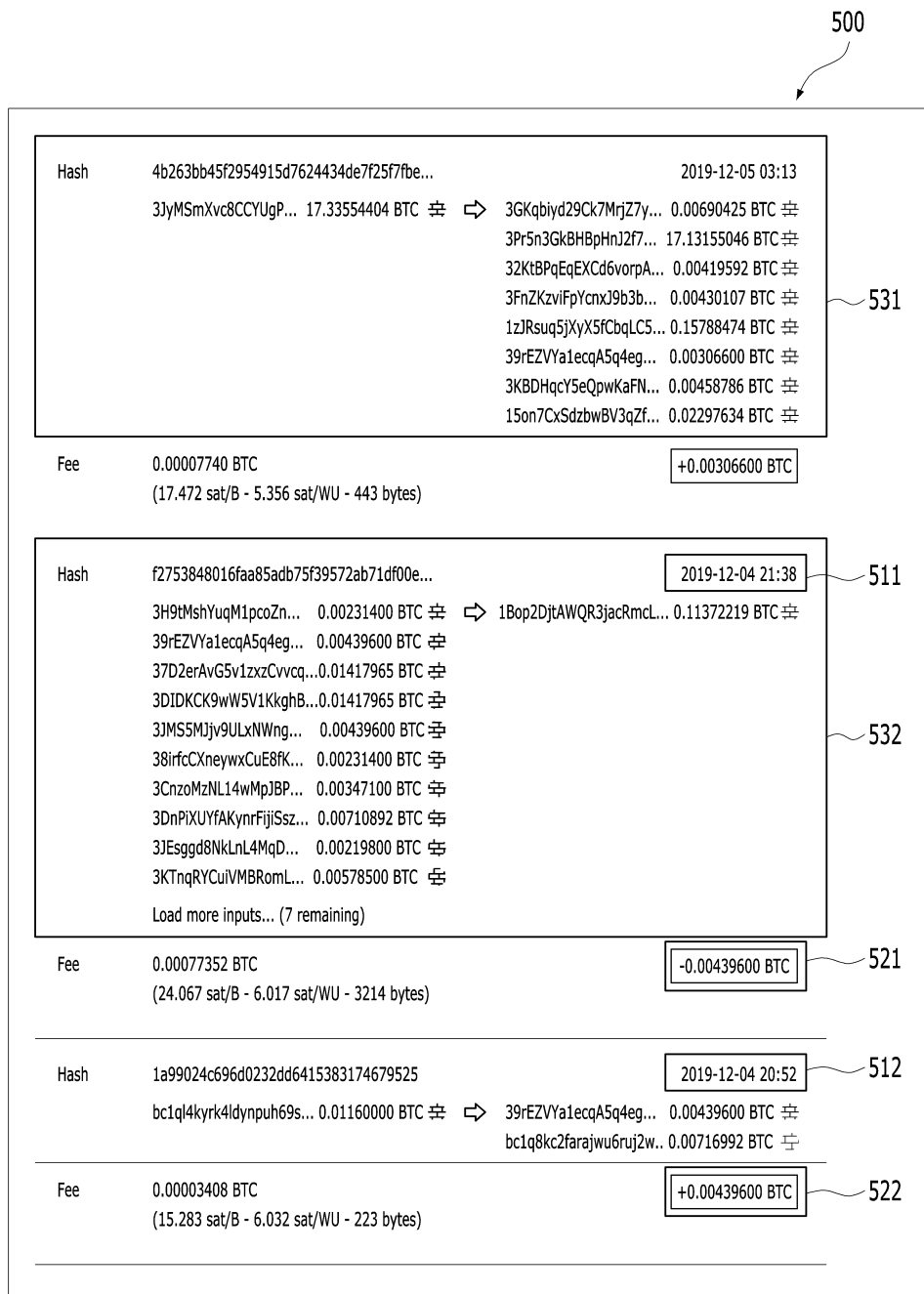
Total Sent 0.30830651 BTC 440

Total Balance 0.00000000 BTC 450

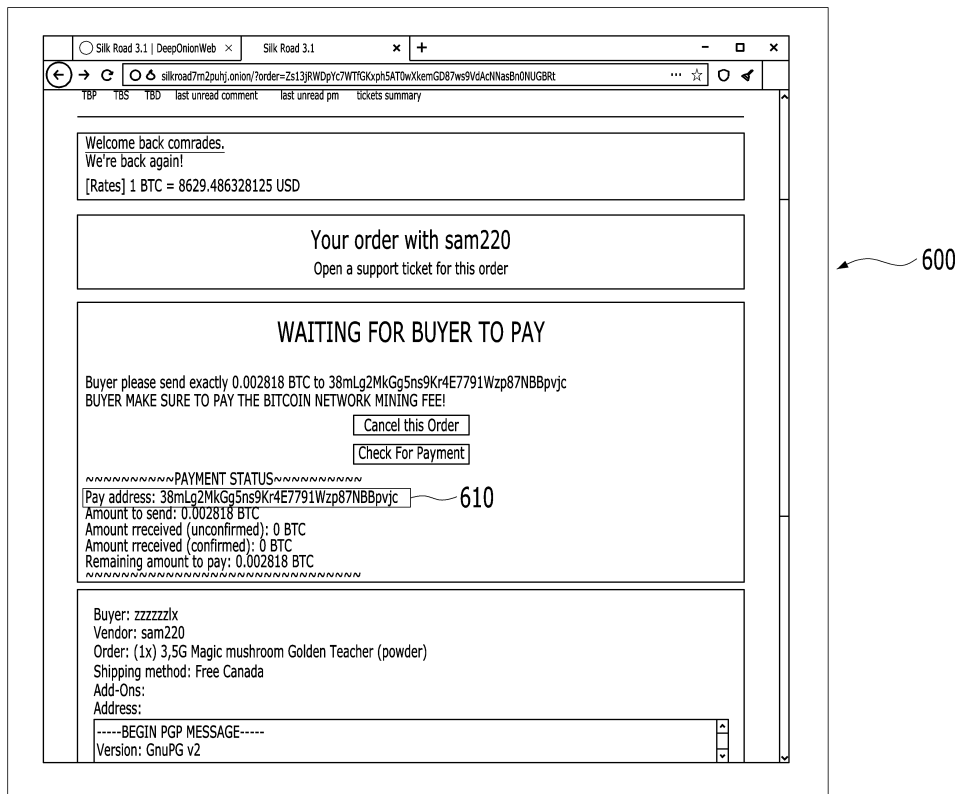
Payment Request

Donation Button

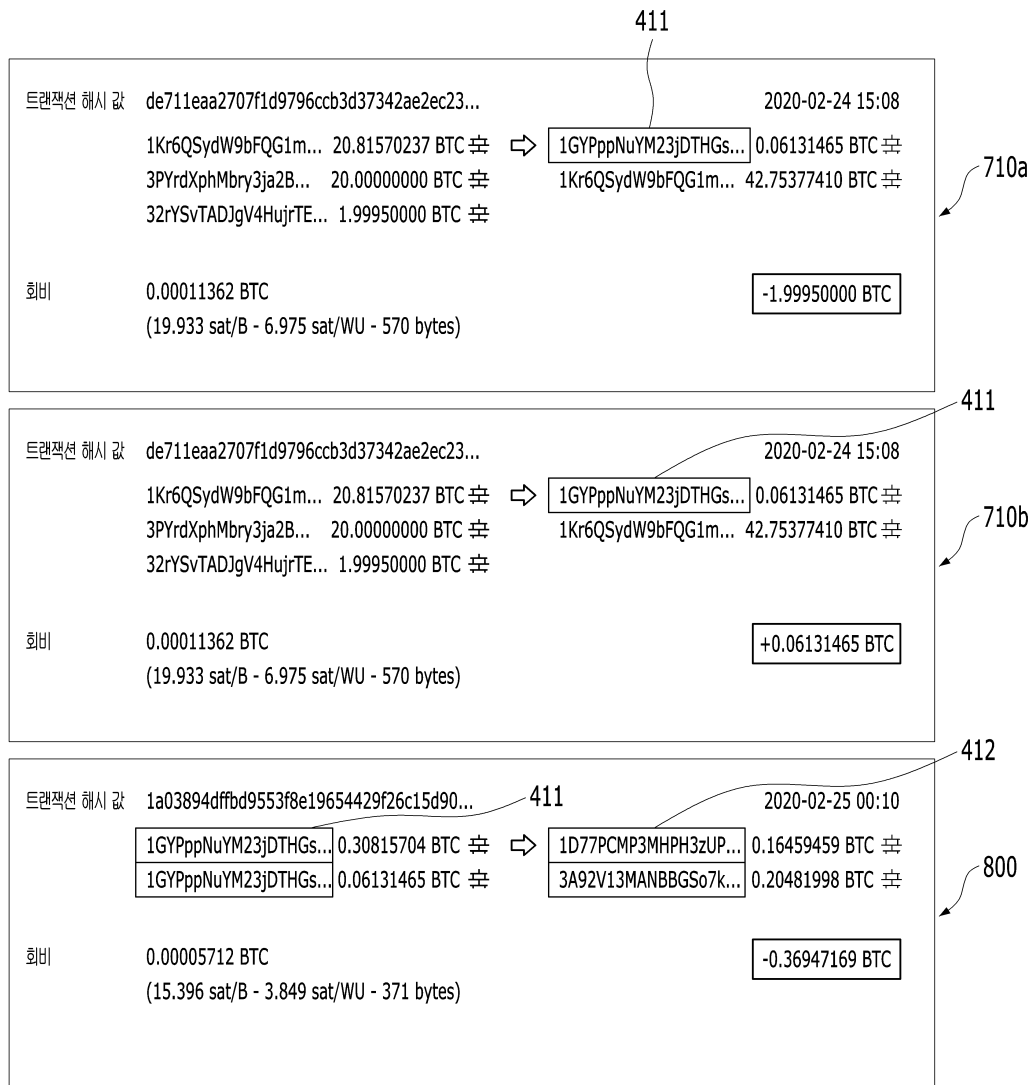
도면4



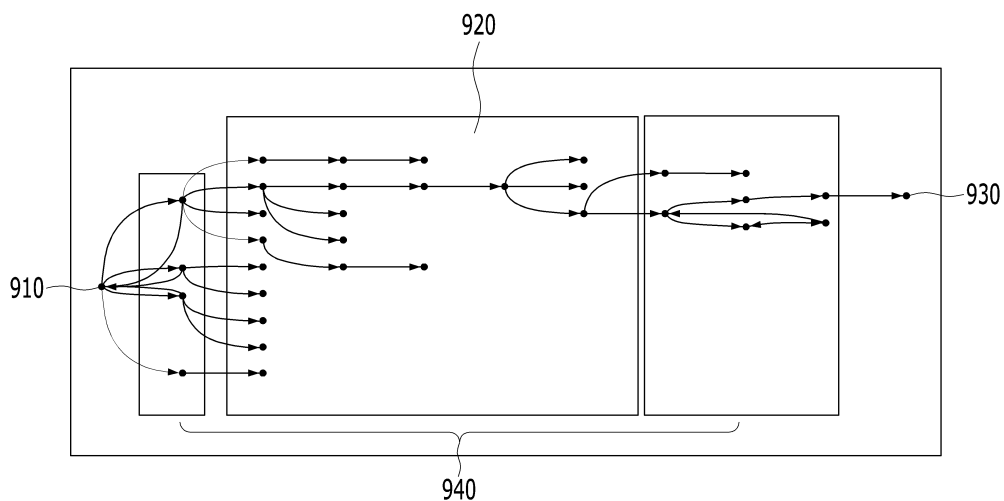
도면5



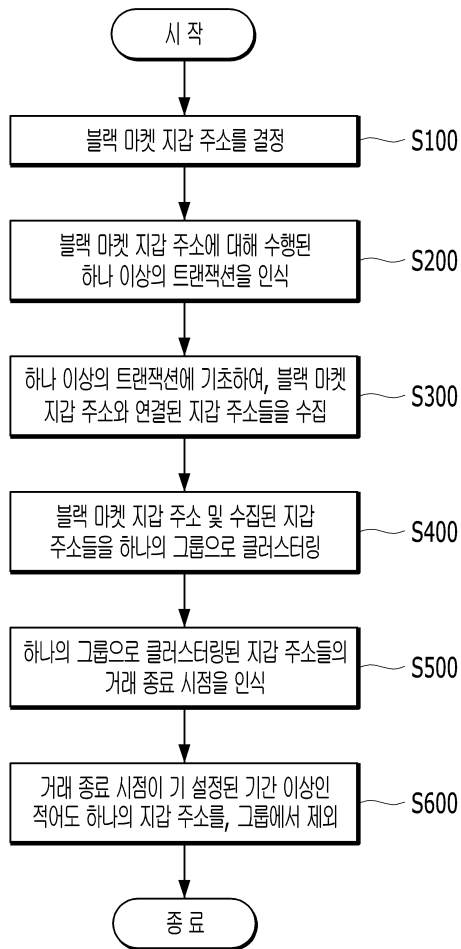
도면6



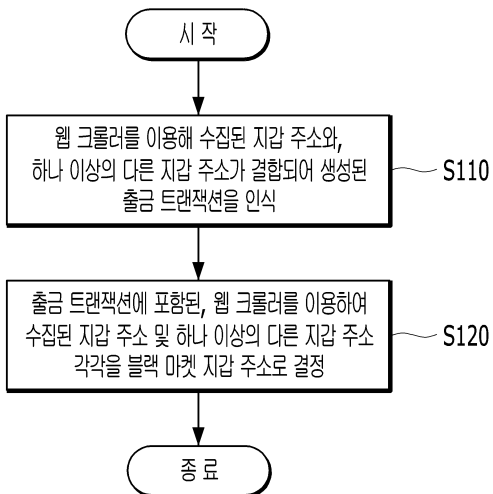
도면7



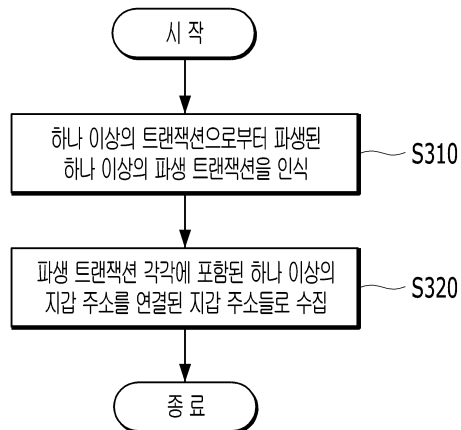
도면8



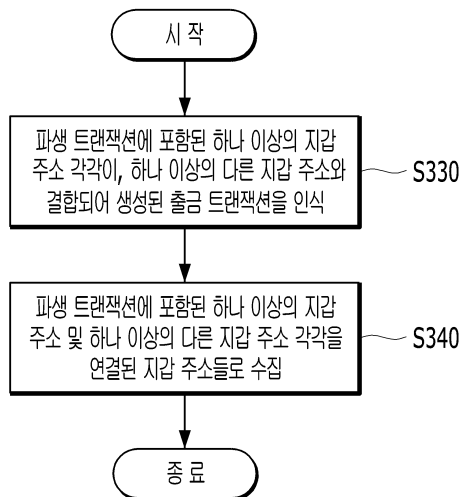
도면9



도면10



도면11



도면12

