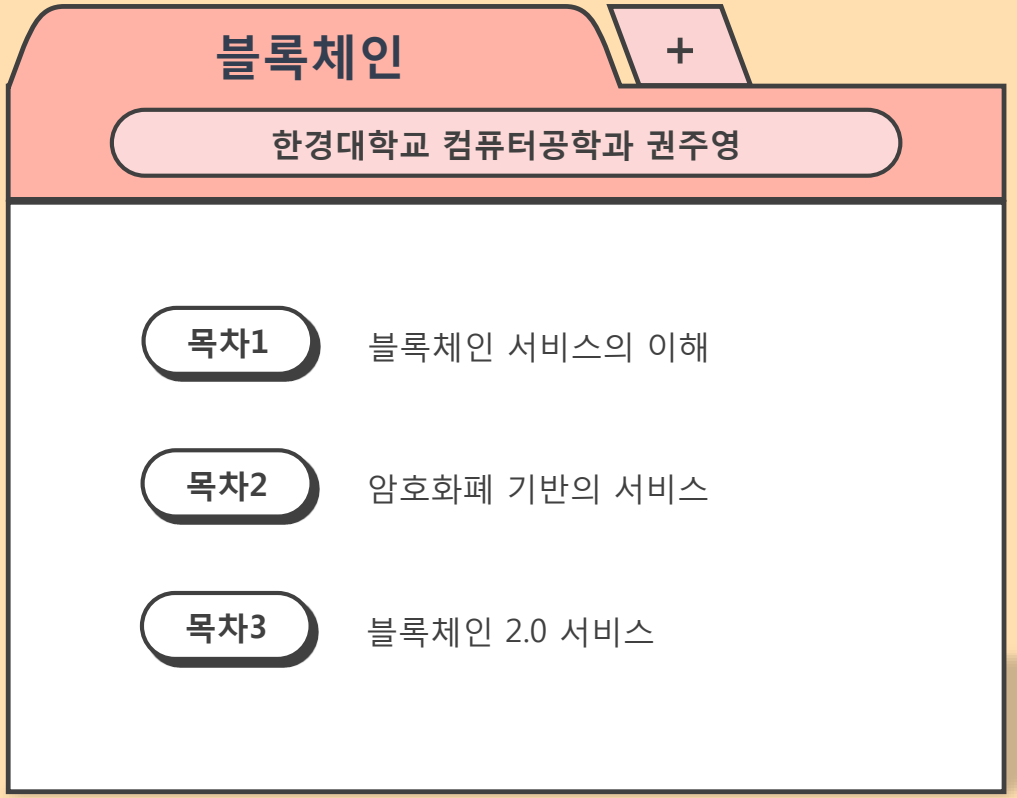
블록체인 +

한경대학교 컴퓨터공학과 권주영

블록체인 서비스 활용하기



블록체인 서비스 활용하기

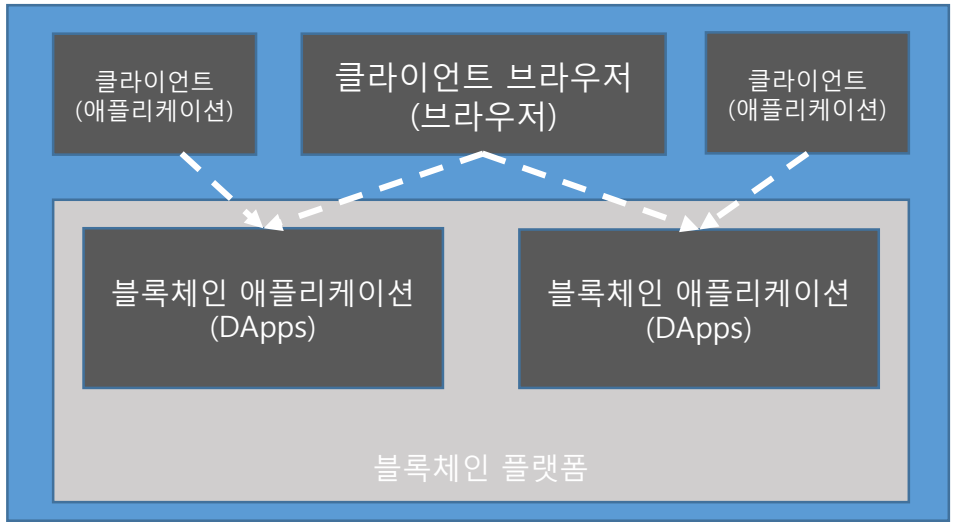
블록체인

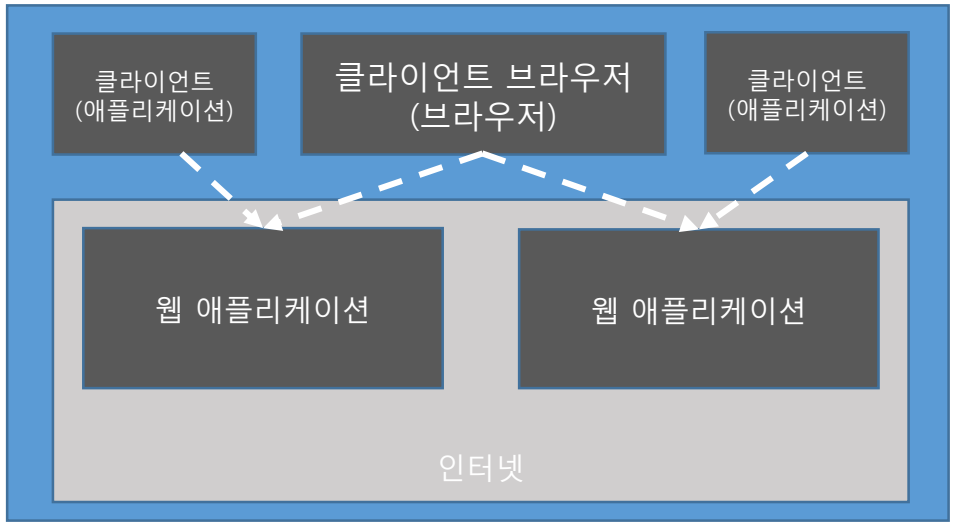
한경대학교 컴퓨터공학과 권주영

1. 블록체인 서비스의 이해

1. 블록체인 서비스의 이해

블록체인 서비스와 웹 서비스 아키텍처 비교





블록체인을 비즈니스에서 활용을 할 때에는 아키텍처의 어느 부분을 사용할지 생각해야 함.

1. 블록체인 서비스의 이해

개발 난이도에 따라 블록체인을 활용하는 방법

기존 암호화폐나 블록체인 서비스를 이용

암호화폐나 블록체인을 활성화하는 서비스 제공

기존 블록체인 플랫폼 안에 새 어플리케이션 개발

새 블록체인 플랫폼 제안 및 개발

1단계
- ✓ 기존 암호화폐나 블록체인 서비스로 수익을 효율화

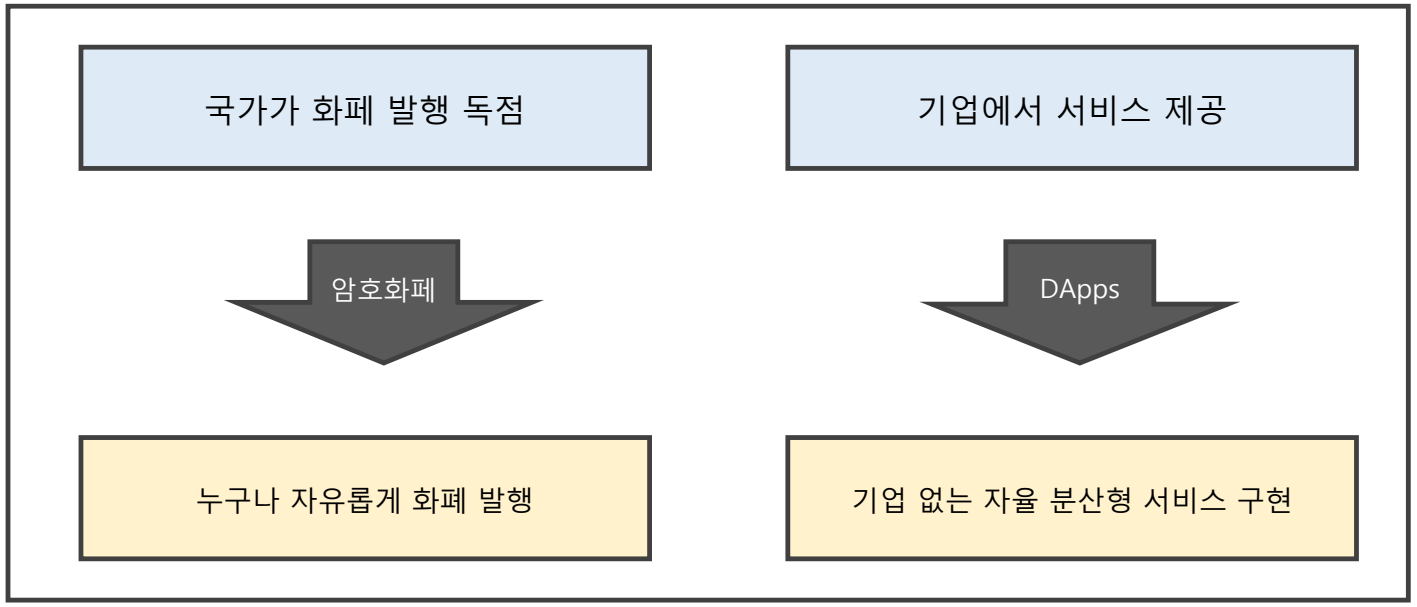
2단계
- ✓ 암호화폐나 블록체인을 사용하겠다는 사람에게 필요한 서비스를 제공, 수익화

3단계
- ✓ 기존 블록체인 플랫폼 안에 새 애플리케이션을 개발해 수익화

4단계
- ✓ 새로운 블록체인 플랫폼이나 기술을 제안, 개발

1. 블록체인 서비스의 이해

새 비즈니스 모델 구축

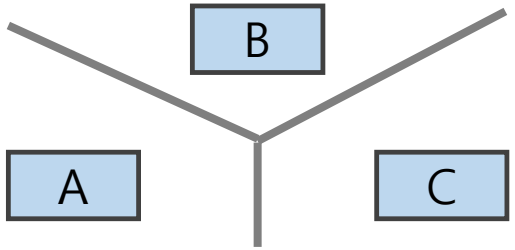


화폐 발행의 자유는 국가가 독점하던 화폐 발행의 이익을 나눈다는 의미

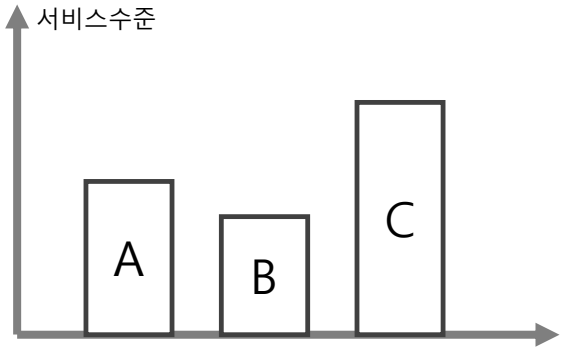
1. 블록체인 서비스의 이해

오픈 소스와 블록체인 – 폐쇄적인 개발 환경과 개방적인 개발 환경

폐쇄적인 개발 환경



회사마다 기초 기술부터 개발

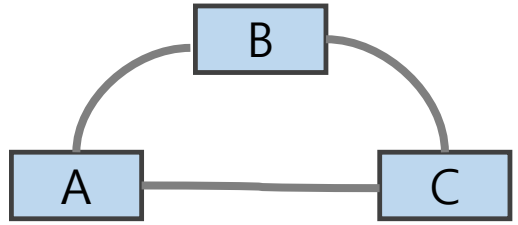


비슷한 기능을 회사마다 재개발

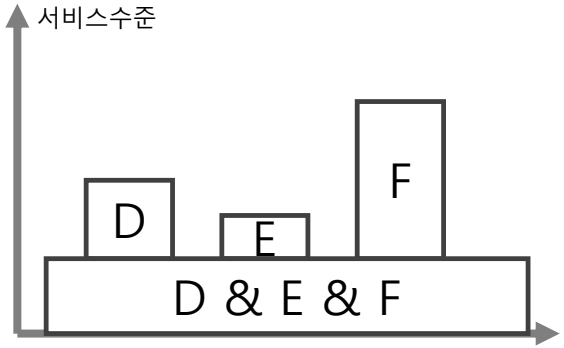
기술 독점에 따른 운영 비용 증가

기밀 유지 비용 증가

개방적인 개발 환경



기초 기술을 공유한
상태에서 부가 기능을 개발



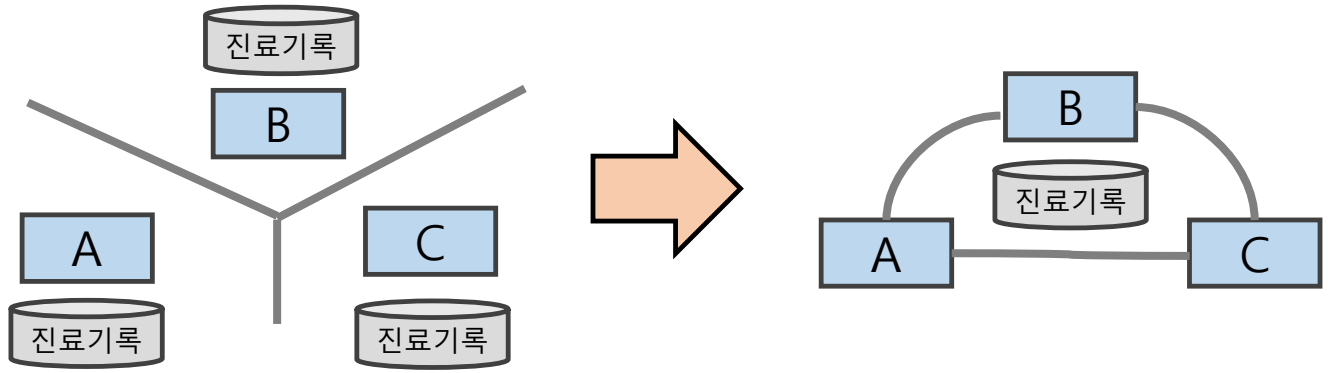
기술 공유로 개발 비용 절감

소프트웨어 품질 향상

부가 기능 개발에 주력

오픈 소스와 블록체인 – 오픈 소스 개발의 혜택

- 오픈소스의 기본 개념 : 집단 지성을 이용하여 소프트웨어의 품질을 높이는 것
- 기초 기술 공유를 통해 기술의 표준화 및 버그 발견율을 높일 수 있다.
- 어느 정도 개발된 소프트웨어에 각 회사마다 필요한 기능을 덧붙여 소프트웨어를 개발할 수 있다.
- 즉 오픈소스는 효율적인 개발 구조를 만들어 비용 절감을 통해 수익을 낼 확률을 높인다.



예) 블록체인을 이용한 병원 사이의 환자 진료기록 데이터 공유

크라우드 펀딩과 ICO

- 새 암호화폐나 블록체인 플랫폼을 개발할 때 자금 확보를 목적으로 ICO(initial Coin Offering)를 발표
- 개발 후 해당 플랫폼의 암호화폐를 발행하거나 현재 소유한 암호화폐를 파는 것

IPO

- 기업이 신규 상장하는 주식을 판매하는 것
- 미래에 투자한 자금을 최대 비율로 회수하기 위해 구매
- 비즈니스 모델로 성공할 확률이 높거나 이익이 높을 것으로 기대되는 프로젝트에 투자

크라우드 펀딩

- 일반인도 부담 없이 소액의 자금을 제공 가능함
- 프로젝트 성공시 소정의 증정품을 받거나 기여한 사람으로 이름을 남기기도 함
- 투자금 회수보다는 프로젝트의 목적과 이념에 공감

ICO

- 새 블록체인 플랫폼 프로젝트의 개발 자금을 받은 후 플랫폼에서 사용하는 토큰을 발행해 줌
- 사회문제를 창업으로 해결하려는 사회 창업가에게 큰 힘이 됨
- 아직 법적으로는 보호받지 못함

블록체인 +

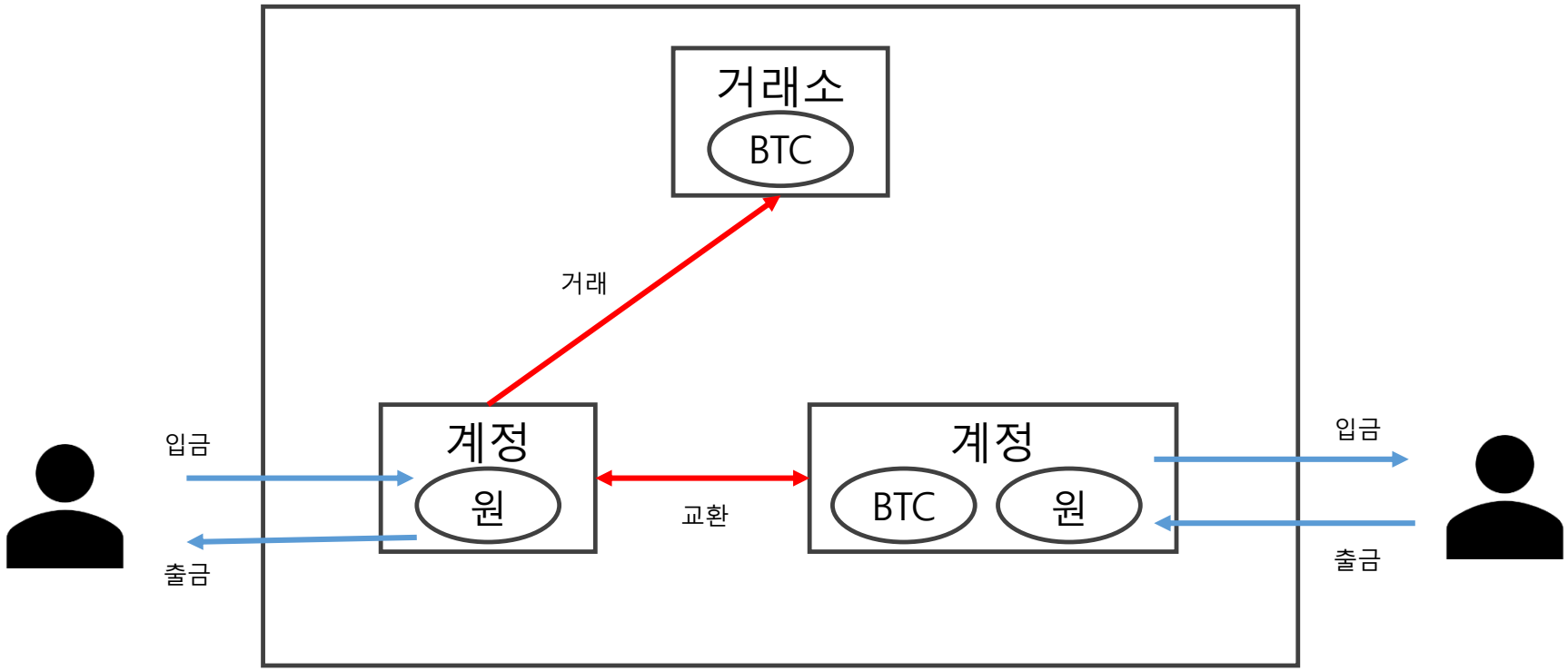
한경대학교 컴퓨터공학과 권주영

2. 암호화폐 기반의 서비스

암호화폐 거래소

- 암호화폐 거래소 : 암호화폐, 법정 통화, 다른 암호화폐를 서로 교환하는 서비스
- 영어로는 'Cryptocurrency Exchanges'
- 암호화폐를 얻는 가장 간단한 방법은 이미 암호화폐를 소유한 사람에게 사는 것

암호화폐 거래소의 개념



탈중앙화 암호화폐 거래소

- 암호화폐 거래소는 특정 회사가 거래소 서비스를 제공한다.
- 회사가 망하게 될 경우 계정에 남은 금액을 모두 잃어버릴 위험이 존재한다.
- 카운터파티 리스크
  - 비트코인 시스템은 중단 없이 계속 동작하더라도, 특정 회사가 제공하는 서비스에 의존하면 문제 발생 확률이 있다.
- 카운터파티 리스크 문제를 해결하기 위해 탈중앙화 암호화폐 거래소 등장
- 계정 등록이 필요 없으며, 본인 확인 절차가 없으며 카운터파티 리스크 발생 확률이 0에 가까움

지갑

- 거래소 계정에 있는 고액의 암호화폐는 '카운터파티 리크스'에 노출될 위험성이 있다.
- 이를 막고자 암호화폐를 안전하게 저장하는 '지갑'이라는 기능이 등장
- 지갑에는 거래에 사용하는 비밀 키를 저장하고 있다.
- 지갑은 비밀 키의 안전한 관리와 거래 편의성을 모두 만족시키는 서비스이자 애플리케이션
- 지갑의 보안 강도는 비밀 키를 온라인/오프라인 어느 쪽에 보관하냐로 구분 가능

지갑 – 뜨거운 지갑

- 뜨거운 지갑은 온라인에 보관하는 지갑이다.
- 암호화폐 거래가 잦으면 즉시 사용 가능하다.
- 데스크톱 지갑
  - PC에 설치하는 애플리케이션 형태
  - PC를 인터넷에 연결하지 않으면 차가운 지갑으로 사용 가능
- 모바일 지갑
  - 스마트폰 앱 형태
  - 스마트폰만 있으면 어디서든 암호화폐 거래 가능
  - 인터넷에 연결되어 있지 않으면 차가운 지갑으로 사용 가능
- 웹 지갑
  - 웹 서비스 형태
  - 거래소 계정에 암호화폐를 보관하는 것이 웹 지갑의 형태
  - 특정 기기에 의존하지 않는다.

지갑 – 차가운 지갑

- 차가운 지갑은 오프라인에 보관하는 지갑이다.

- 종이 지갑
  - 비밀 키 문자열이나 QR 코드를 종이 형태로 출력한 것
  - 암호화폐를 오랫동안 보관할때 사용하면 좋음
  - 지폐처럼 타인에게 양도 가능
  - 한번 인쇄된 문자열이나 QR 코드는 수정 불가능
  - 단점으로는 문자열이나 QR 코드가 다른 사람에게 노출될 수 있다.

- 하드웨어 지갑
  - 비밀 키를 보관하는 용도로 만든 기기(OTP 기기와 비슷)
  - 기기을 잃어버리더라도 비밀 키를 보호할 수 있다.

- 뇌 지갑
  - 사람이 기억하기 쉬운 문장 등으로 비밀 키를 생성한 후 사람이 기억하는 것
  - 가장 강력한 비밀 키 보관 방법이지만, 임의 문자열을 실수 없이 기억하는 것은 거의 불가능
  - 따라서 기억하기 쉬운 문장으로 비밀 키를 생성

암호화폐의 결제

- 사용자의 장점
  - 암호화폐는 물리적인 지갑 등에 화폐를 넣어 관리할 필요가 없다.
  - 스마트폰 등의 기기로 보낼 곳의 주소를 QR 코드 등으로 읽고 결제할 금액을 보내면 된다.
  - 법정 통화와 달리 전 세계 어디에서나 사용 가능, 사용 한도에 제한이 없다.

- 상점의 장점
  - 모든 거래 내역 보관을 디지털화 하여 거래 내역과 실제 금액이 일치하지 않는 문제를 막을 수 있다.
  - 물리적인 현금 관리 인적 비용을 절감할 수 있고, 도난 등의 위험도 막을 수 있다.

- 암호화폐 결제 도입과 해결 과제
  - 암호화폐를 결제 수단으로 도입할 때 보통 암호화폐 지갑의 주소를 이용
  - 암호화폐 결제 서비스를 사업화 하려면 납세, 법정 통화와 교환, 암호화폐 가격 변동 대응 등 여러가지 상황을 고려해야 함

암호화폐 결제와 송금 서비스

- 지갑
  - 결제나 송금이 잦은 모바일 지갑 및 웹 지갑 등은 잔액확인, QR 코드로 주소 읽기, 적절한 수수료 설정 기능 등을 제공
  - 일부 지갑은 자주 거래하는 상대를 주소록에 등록해 QR 코드 없이 이체 가능

- 암호화폐 직불 카드
  - 이미 사용 중인 결제 서비스에 암호화폐를 도입해 결제하는 방법
  - 현재는 과도기 적인 서비스

- 믹싱
  - 암호화폐 주소에 있는 정보로 어느 정도 개인 정보를 추측할 수 있다.
  - 이 문제를 해결하는 방법으로 믹싱 서비스를 이용
  - 여러 사람의 거래를 무작위로 처리하는 거래 풀을 이용, 거래 추적을 어렵게 만듦

암호화폐 결제와 송금 서비스

- 꾸밈 주소
  - 암호화폐 주소를 사람이 기억할 수 있는 가독성 높은 문자열로 생성하는 방법
  - 자신이 원하는 문자열이 포함된 주소 형식을 입력한 후 연산 작업으로 그에 맞는 주소와 비밀키를 발견하는 작업
  - 예를 들어 비트코인 표준 주소는 '1'로 시작해서 '0', 'O', 'I', '1'을 제외한 58개의 숫자 및 알파벳으로 구성된 27~34개의 문자열

패턴	난이도	비트코인 주소 예	연산시간(1Mkey/s)
1	1	169biqrJCphnzUjyu1Gvv5jRMTEcxBb8jc	1초 이하
1V	1353	1V4q3wPtcGV3UmCkTmQkBHGf7h2fHKXqn	1초 이하
1Va	78508	1VaFb2RiVZ1ZfNfJf1CoZEfaVmAxsKuyP	1초 이하
1Van	4553521	1Van4JcuZkWc96PfC48WxQtXX4EiYcMPN	10초
1Vani	65104224	1Vanicvyu3yq9B4Wp1fXY3fLomnm1xnQk	5분
1Vanit	15318045009	1VanitLmzFVj8ALj6mfBsifRoD4miY36v	3시간
1Vanity	888446610538	1VanityN7fntA2xmN7WPYutHMrtGDe2Sr	1주

암호화폐 결제와 송금 서비스

- 블랙리스트
  - 암호화폐를 사기에 악용하는 경우
  - 스팸 메일 등으로 특정 주소에 송금을 재촉 시 해당 주소를 블랙리스트에 등록해 송금하지 않도록 알릴 수 있다.

- 매칭
  - 거래를 하고 싶은 사람과 서로 연결하여 안전 거래를 실현
  - 탈중앙화 암호화폐 거래소가 매칭 서비스의 예

암호화폐 플랫폼에 기여하기

- 채굴
  - 채굴에 성공하면 새로운 암호화폐를 발행할 권리를 제공하거나 거래 수수료를 받을 수 있다.
  - 채굴에 협력하는 사용자가 많을수록 암호화폐 플랫폼의 보안성이 강화된다.
  - 3가지의 채굴방법
    - 단독 채굴
      - 혼자 채굴에 참여, 채굴에 필요한 모든 요소를 본인이 운영하지만 얻는 보상은 모두 자신의 소유
    - 채굴 풀
      - 여러 사용자가 참여, 서로 다른 사람이 채굴 할 때 낮은 채굴 성공 확률이라는 단점을 보완하고 성공 보상을 사용자에게 나눈다.
      - 보상은 낮지만 안정적으로 받을 수 있다.
      - 단독 채굴과 같이 각 사용자가 하드웨어 구축, 운영, 전기 요금 납부 등을 함
    - 클라우드 채굴
      - 채굴 사업자가 크라우드 펀딩으로 구축 및 운영 자금을 모은 후 클라우드 방식으로 채굴 후 성공 보상을 분배
      - 펀딩에 참여했다고 꼭 보상을 받을 수 있는 것은 아님

암호화폐 플랫폼에 기여하기

- 수확
  - 알트체인 'NEM'에서 제시한 블록 생성 방법
  - 암호화폐 거래량(기여도)에 따라 블록을 생성해 보상을 지급
  - 특별한 하드웨어를 구축하지 않고도 거래만 활발하면 보상을 얻을 수 있다.

- 차익 거래
  - 복수의 암호화폐 거래소 사이의 교환 비율 차이를 이용해 이익을 남기는 것

블록체인 +

한경대학교 컴퓨터공학과 권주영

3. 블록체인 2.0 서비스

블록체인 2.0 서비스

- 광고 서비스
  - 브레이브(Brave)라는 브라우저를 통해 개인정보를 추적하지 않는 광고만 보여주며, 누구나 광고 표시 여부를 선택할 수 있다.
  - 암호화폐로 광고 수익을 받아 콘텐츠 제공자, 네트워크 사업자, 사용자에게 나누는 모델을 제안
- 예측 서비스
  - 참가자들이 미래의 사건을 예측한 후 실제 결과에 따라 배당금을 받는 것
- 자산 관리 서비스
  - 자산 내역들을 블록체인에 저장해 관리
- 현금 대출
  - 블록체인에서 디지털로 관리하는 실제 자산을 담보로 현금을 대출하는 서비스가 있다.
  - 이를 통해 대출 금리를 낮출 수 있다.
- 분산 동영상 서비스
  - 블록체인을 이용하여 동영상 제작자나 권리자에게 직접 동영상 시청 수익을 전달
  - 미리 설정한 수익 분배율에 따라 스마트 계약으로 수익을 나눈다.

기타 블록체인 2.0 서비스

- Storj
  - 블록체인을 이용한 분산 저장공간 공유 서비스
- 골렘
  - 블록체인으로 분산 슈퍼컴퓨터를 구현하는 프로젝트
  - 개인이 소유한 CPU나 GPU등의 연산 자원을 제공하면 보상으로 암호화폐 지급
- 메모리체인
  - 디지털 토큰 대신 암호화폐 개념인 거래 카드를 발행해 교환하는 플랫폼
  - 블록체인을 이용해 디지털 데이터에 소유권을 부여하여 마음대로 데이터를 복제할 수 없는 환경을 만든다는 목표
- 크립토키티
  - 이더리움 기반 스마트 계약으로 만든 '고양이' 육성 시뮬레이션 게임
  - 게임상의 고양이는 토큰, 따라서 같은 고양이는 세계에서 단 한 마리만 있다.

블록체인 +

한경대학교 컴퓨터공학과 권주영

감사합니다