12차시. 블록체인과 사이버 보안

01. 블록체인의 이해

블록체인의 개념

블록체인과 비트코인

블록체인이라고 하면 비트코인을 먼저 떠 올리는데 이것은 블록체인이 비트코인의 거래 기록 기술로 구현되었기 때문이다. 블록체인을 학습하기에 앞서 블록체인과 비트코인의 관계를 알아보자. 블록체인은 비트코인의 운영 체계이고, 비트코인은 블록체인을 화폐 발행과 운영에 응용한 것이다. 따라서 핵심이 되는 기반 기술 체계는 블록체인이고, 비트코인은 블록체인에서 생성된 서비스의 하나로 파악하면 된다.

잠깐!

비트코인은 완전히 가상적이고 무형의 것인가?

- 비트코인은 신용카드나 온라인 뱅킹과 같이 가상(virtual)의 특성을 지님
  . 비트코인은 온라인은 물론 물리적인 상점에서 사용 가능
  . 카사스시우스(Casascius)코인과 같이 물리적 형태로 교환 가능
  . 비트코인 잔고는 분산네트워크에 저장되어 사기 행위 차단
- 비트코인 사용자는 자신의 펀드(fund)에 대해 전적인 통제권을 보유하며 가상이라는 이유로 소멸되지 않음

카사스시우스

- 비트코인 지지자이자 소프트웨어 엔지니어인 마이크 캘드웰이 여러 가지 금속재료로 직접 만든 비트코인 동전
- 캘드웰은 2011. 9월 7가지 디자인으로 직접 비트코인을 실체화. 실체가 없어 대중성화되지 못하고 있다고 판단해 형체를 만듦. 캘드웰은 각 동전마다 고유 식별키를 부여하고 홀로그램 스티커도 부착.
- 영어로 “솔직히 말하다(call a spade a spade)”라는 뜻의 문장 앞 글자를 따서 만든 것.

블록체인의 개념

블록체인의 분산원장(shared ledger)은 인터넷에서 서로 알지 못하는 다수의 상대방과 거래를 할 때 중개기관의 개입 없이 서로 신뢰할 수 있도록 만들어주는 탈중앙화된 정보공유 저장기술 이다. 기존 금융시스템은 원장을 집중 관리하는 신뢰할 수 있는 제3의 기관을 설립하고 해당기관에 대한 신뢰를 확보하여 금융거래를 하는 방식으로 발전해 왔다. 특히 온라인 금융시스템에서는 페이팔과 같은 제3의 사업자가 거래자에 대한 신상정보 및 잔액 등의 장부를 관리하고 이용자는 수수료를 지급했다. 이러한 신뢰 비용은 사용자들의 부담으로 고스란히 전가되는 것이다.

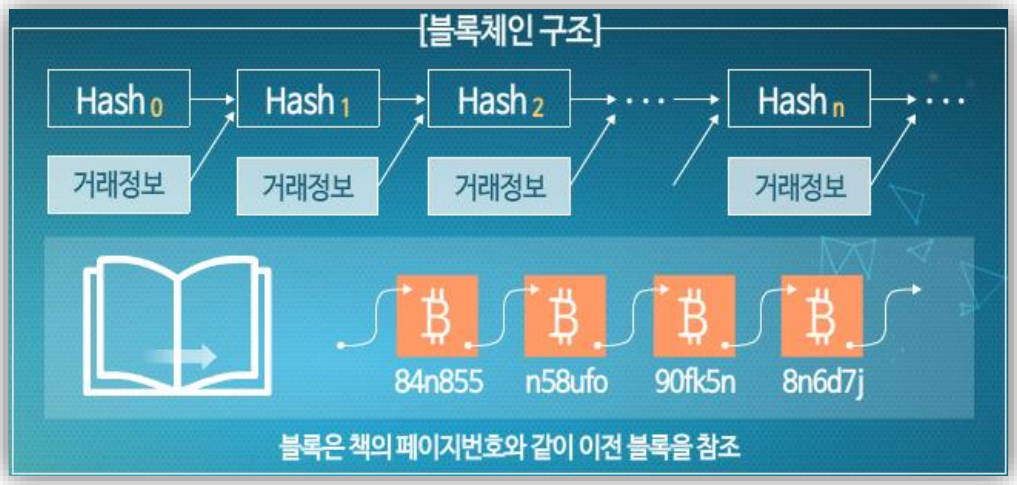
분산원장기술은 사용자간 상호 신뢰를 할 수 있도록 설계된 시스템이다. 이를 위해 분산원장기술은 모든 개인 간의 거래를 포함하는 원장을 모든 구성원이 갖고 있는 분산저장 시스템을 구현했다. 어떤 순간이고 모든 구성원이 같은 장부를 갖고 있는 것을 입증할 수 있다면 이를 조작하는 것이 사실상 불가능하여 신뢰할 수 있다. 이를 위해 특정시간 단위로 블록이라는 단위의 거래장부를 생성하고 이를 모든 구성원에게 전송하여 다수의 구성원이 거래의 타당성을 검증하고 전송된 블록의 유효성을 승인할 경우 모든 구성원이 각자 분산관리하는 원장 즉 기존의 거래 블록 페이지 끝에 새로운 블록을 체인형태로 연결한다. 이렇게 해서 모든 구성원이 같은 분산원장을 갖게 한다.

이렇듯 분산원장으로 설계되고 구현된 시스템은 공통의 장부를 관리하는 다수의 네트워크 참여자가 거래 타당성을 검증하고 이를 승인해야 거래가 성립된다. 이 시스템은 중앙 중개기관의 개입 없이 사용자 간(P2P: Peer-to-peer) 직접적인 거래가 가능하도록 참여자들에게 상호 신뢰를 주도록 정책적인 장치가 설계되어 있다. 결론적으로 분산원장기술은 전통적으로 신뢰가 없는 네트워크 상에서 사용자들의 부담으로 고스란히 전가되는 신뢰비용을 최소화하고 익명의 상대와 거래를 할 수 있는 기반기술이라고 정의할 수 있다.

블록체인의 특징

- 거래기록 위변조 방지

블록체인은 모든 거래기록 내용을 한 곳에 저장하는 것이 아니라 모든 참여자의 장부에 기록하는 방식이다. 이러한 블록체인의 원리는 비트코인 거래 기록의 위변조를 방지하는 목적으로 활용된다. 비트코인의 블록체인 구조를 살펴보면, 이전에 기록한 내용의 요약내용(해시값 형태)과 기록시간인 '타임스탬프'를 포함하고 있다. 아울러 새롭게 추가된 거래 내용은 해시의 형태로 저장하고 해시 자체에 대한 해킹을 막기 위해서 임의의 변수인 '난수(Nonce)' 값을 추가한다.



블록체인은 거래 기록을 주기별로 끊임없이 상호간에 매핑한다. 거래 기록 중 불일치하는 부분이 있으면, 다수 원칙에 따라서 위변조 된 기록을 찾아낸다. 이는 해커가 기록을 위변조 하는 것을 거의 불가능하게 만든다. 기록 정보를 서로 매핑하는 과정에서 개인의 컴퓨팅 파워를 이용한다. 그래서 이미 모든 참여자에게 기록한 정보를 해킹하기 위해서는, 모든 참여자의 50%를 넘는 컴퓨팅 파워를 이용해야 한다. 그래서 블록체인은 참여자가 많을수록 데이터 위변조가 어려워진다고 볼 수 있다.

- 탈중앙화와 공유

불과 3년 전까지만 해도 블록체인은 비트코인의 기반기술로만 인식됐지만 블록체인이 가진 거래 기록 보안성 이외에 추가적인 특징이 발견되면서 다양한 산업에서 주목받기 시작했다. 즉, 탈중앙화 특징과 공유 특징이다.

· 탈 중앙화: 탈 중앙화 특성으로 중개에 따른 비용을 줄 일수 있다. 기존의 중앙 집중형 방식은 서비스 수요자들을 관리하는 중개자가 항상 있었다. 국제 환전을 예로 들면, 각국의 은행 사이에 스위프트(SWIFT)라는 중앙 관리기관을 거쳐야 한다. 스위프트가 각국의 은행에서 일어난 거래 기록을 관리하기 때문이다. 그러나 블록체인 방식은 스위프트가 필요 없다. 거래기록이 은행(참여자) 시스템에 자동으로 등록되기 때문이다. 이는 중개기관에서 처리하는 시간과 수수료를 절감시킨다. 액센츄어가 거대 은행 기업 10곳을 대상으로 블록체인 적용 효과를 조사한 결과, 블록체인은 기존 은행간 거래에서 발생하는 비용을 약 30% 가량 절감시키는 것으로 나타났다.

잠깐!

SWIFT(Society for Worldwide Interbank Financial Telecommunication) 국제 금융거래신경망

- 200개 이상 국가, 11,000,개 금융기관에서 사용하는 SW와 서비스 제공
- SWIFT 메시지 해킹: 2016. 2월 발생

. 사건 경위: swift 메시지 조작(은행원들이 보는 화면 상에서는 거래상 금액을 변조)하여 뉴욕연방준비은행 방글라데시 계좌에서 8,100/2,000만 달러 이체

· 공유: 블록체인은 '공유'라는 특징을 갖고 있다. 블록체인 원장은 참여자 모두에게 실시간으로 공유되기 때문에 정보가 공유된다고 할 수 있다. 정보는 기관에 따라 개별 운영되었지만 블록체인 방식은 모든 정보를 개별로 저장하게 하는 것이 아니라 모두 저장하게 하여 업무 협업능력을 향상시킬 수 있다.

예를 들어 A 기관에서 발생한 정보를 관련 기관 전체에 공유하기 위해 A는 B의 양식에 맞춰서 정보를 저장하고 공유해야 했다. 이 경우 정보 공유를 원하지 않을 때 정보를 숨길 수 있고 정보 저장에 양식을 맞춰야 하기 때문에 비용을 야기할 수 있다. 하지만 블록체인 방식은 이러한 문제를 해결한다. 정보가 생성되면 시간 주기에 따라 자동으로 공유되기 때문이다. 아울러 정보 저장방식도 표준으로 이미 제공된다. 이는 정보 공유에 있어서 기관별로 정보 공유의 어려움을 해소한다.

이는 고객에게 제공하고자 하는 정보를 빠르게 제공할 수 있다. 현재 월마트는 IBM과 중국 칭화대학교와 함께 블록체인 기반의 '식품유통이력관리' 사업을 진행하고 있다. 식품유통이력관리는 유통에서 발생하는 식품이력 내용을 블록체인에 저장해 유통 참여자들이 서로 볼 수 있게 하는 서비스이다. 아울러 소비자가 원할 때도 식품이력을 볼 수 있게 한 번에 제공한다. 기존에는 식품유통이력관리가 개별로 기록되었다면, 블록체인으로 모든 이력관리가 블록체인에 함께 기록된다. 이는 식품유통에 문제가 발생했을 때 빠르게 대처할 수 있게 한다. 월마트는 식품유통 관리시스템을 일부 구축하고 시연했었다. 시연 결과, 한 유통 과정에서 발생하는 모든 이력을 불러오는데 2.6초 밖에 걸리지 않았다

결론적으로 블록체인은 위변조 방지, 탈 중앙화, 공유의 특징으로 단순히 비트코인 기반 기술이 아닌 신성장동력 기술로 세계적으로 주목받고 있는 것이다. 블록체인의 선두주자인 IBM은 블록체인이 인터넷만큼의 영향을 미칠 것이라고 홍보하고 있다. '유엔 미래보고서 2050'는 10대 유망 기술 중 하나로 블록체인을 꼽았다. 다양한 산업은 물론 국가의 전자정부에도 블록체인이 적용될 전망이다.

블록체인의 유형

분산원장기술을 구분하는 방법은 여러 가지가 있지만 그 중 가장 대표적인 것은 참가자들의 자격을 제한하는 정도에 따라 퍼블릭과 프라이빗 분산원장으로 분류한다. 퍼블릭 분산원장 시스템은 다른 참가자들의 허용 없이 누구나 분산원장에 읽고 쓸 수 있기 때문에 '퍼블릭'이며 누구도 그 권한을 부여받거나 부여하지 않는다. 반면 '프라이빗' 분산원장 시스템은 미리 정해진 참여자만이 네트워크에 접속하여 정해진 권한만을 이용하거나 행사하게 된다.

- 퍼블릭 분산원장 시스템: 퍼블릭 분산원장 시스템은 누구나 원하기만 하면 네트워크에 접근하여 거래내역을 읽거나 제출하거나 또는 거래를 검증하고 생성할 수 있도록 한다. 이런 시스템에서의 블록체인은 경제적인 인센티브를 동반하는 작업증명(Proof of Work)의 수단을 사용한 암호 검증으로 안전성이 보증된다. 일반적으로 퍼블릭 분산원장은 참여자들이 익명으로 참여할 수 있도록 되어있고 거래를 검증하거나 참여자간의 합의를 도출하는 등 블록체인을 유지하기 위해 참여자들에게 통화의 발행이라는 인센티브를 제공한다. 예로는 비트코인, 이더리움 등 암호화통화가 있다.

잠깐!

작업증명(Proof of work)
새로운 블록을 블록체인에 추가하려면 새로운 블록에 대해서 정해진 조건의 블록 해쉬 값을 계산하도록 요구하는데 이때 정해진 조건을 구하는 행위를 작업증명이라 함.

- 프라이빗 분산원장 시스템: 프라이빗 분산원장에는 개별 기업이 운영하는 분산원장시스템과 컨소시엄이 운영하는 분산원장시스템이 있을 수 있다. 개별 기업이 자신의 원장관리를 위해 운영하는 시스템은 중앙의 서버가 개별 참여자의 접근과 권한을 승인하는 형태이다. 대표적인 애플리케이션으로는 항공회사의 분산 데이터베이스 관리 시스템이 있다. 항공사는 전 세계의 여행사와 연동하여 고객데이터와 탑승 스케줄 등을 관리한다. 일반적으로 특정 기업이 사용하는 이러한 분산 시스템은 거래를 하거나 혹은 거래검증을 위한 시스템을 운영하거나 참여자간의 합의를 도출하거나 하는 프로세스를 만들거나 내부 화폐를 발행할 필요가 없다.

다수의 기업 혹은 컨소시엄이 운영하는 프라이빗 분산원장 시스템은 미리 지정된 개인이나 단체가 참여자간의 합의 프로세스를 검증하는 권한을 갖는다. 예컨대 금융기관의 컨소시엄 등이 운영하는 분산원장 시스템은 참여자가 제한되고 이들의 권한과 접속이 제한되는 형태로 운영된다. 따라서 부분적 탈중앙화된 시스템이다. 이 형태는 특히 금융기관들이 선호하는 시스템으로 사용자들의 아이디는 고객확인제도(흔히 업무파악의무와 고객파악의무로 지칭되는 금융기관의 의무 사항)를 따르는 것이 필수 사항이 될 수 있다.

02. 블록체인의 활용

여러 기관에서 블록체인이 전 세계에 미칠 영향력은 매우 클 것으로 전망하고 있다. 유엔 미래보고서 2050은 블록체인을 10대 유망기술 중 하나로 선정했다. 2015년 세계경제포럼(WEF - World Economic Forum)에서는 블록체인이 시장에 미칠 영향력을 조사했다. 조사대상은 IT전문가 800명이다. 응답자의 58% 응답자가 2025년까지 GDP의 10%가 블록체인과 관련한 것이라고 답했다. 이 같이 응답한 이유는 블록체인은 플랫폼 기술이기 때문이다. 다시 말해 4차 산업혁명 시대에 ICBM과 함께 여러 산업에 미칠 것으로 전망되기 때문이다.

금융 분야

- **시간과 수수료 절감**

블록체인 출발점 자체가 금융이기 때문에 블록체인이 가장 잘 발달한 분야는 금융분야이다. 블록체인이 금융 분야에서 주목받게 된 이유는 비트코인과 이더리움에서 찾을 수 있다. 사실 비트코인과 이더리움을 분석하면 금융 분야뿐만 아니라 전 산업이 주목받게 된 주된 이유를 알 수 있다. 블록체인의 형태를 가장 잘 구현한 것이 비트코인과 이더리움이기 때문이다.

가장 처음으로 생겨난 블록체인 가상화폐 '비트코인'은 어떻게 주목받게 되었을까? 답은 사람들이 많이 사용하면서 화폐로서 가치를 인정받게 된 것이다. 그렇다면 블록체인이 주는 핵심은 무엇일까? 답은 국가적인 장벽 없이 사용할 수 있다는 것이다. 비트코인은 국가를 초월한 가상화폐이기 때문이다. 여행자의 경우 환전하는 데에 필요한 시간과 수수료를 절감시켜 준다. 이러한 이점을 착안한 은행들은 '비트코인'에 집중하기 시작한 것이다. 다시 말해 서로 다른 통화 이용에 불편한 거래를 가상화폐로 없애고자 한 것이다.

영국 바클레이 은행은 미국 서클(서클 인터넷 파이낸셜)과 제휴를 맺어서 미국과 영국 간에 무료로 송금 및 결제를 할 수 있게 하는 시스템을 2016년 4월에 개발했다. 기존에는 환전 수수료가 들었고 기간도 오래 걸렸지만 이번 서비스로 인해서 환전 수수료가 전혀 들지 않게 했고 기간도 크게 단축시켰다. 운영원리는 비트코인을 매개로 환전을 한 것이다. 영국에서 미국으로 파운드를 달러로 바꿔서 송금한다고 가정해보자. 바클레이는 파운드를 입금 받으면 그 돈을 비트 코인으로 환전하고 비트코인을 다시 미국 달러로 환전해서 미국에 있는 사람에게 전달한다. 비트코인과 명목화폐인 파운드와 달러간의 환전 수수료가 거의 들지 않는 것을 활용한 것이다.

비자는 2015년 10월에 블록체인 스타트업인 'Chain.com'에 투자했다. 그 결과로 Chain.com은 'Chain OS'라는 블록체인을 개발하였다. Chain OS는 금융 서비스에 최적화된 블록체인으로 초당 거래 처리량이 블록체인의 10,000배이다. 블록체인은 거래 처리량이 6 건에서 7건인 반면에 Chain OS는 약 초당 65,000개의 거래를 처리할 수 있다. 현재 금융 서비스 외에 다른 산업에도 적용할 수 있는지 여부에 대해서는 검토 중이다. 정리하면 금융 분야에서 블록체인 산업이 주목받고 있는 이유는 거래와 운용비용 감소이다. 스위프트는 2016년 5월 보고서에서 증권거래 시스템 에 블록체인을 도입하면 기존 대비 약 46조 7천억 원을 줄일 수 있다고 분석했다.

개인간 전력 거래 분야

- **보안과 효율성 제고**

블록체인을 개인 간 전력 거래에 활용할 수 있다. 개인 간 전력 거래 시스템은 전력을 개인 간에 사고 팔 수 있게 한다. 신 재생에너지 도입 확산으로 일반 사용자도 전력 생산이 가능해짐으로서 전력을 판매할 수 있는 것이다. 전력 거래 활성화는 국가 전력 관리의 효율성을 더욱더 향상시키는 역할을 한다. 국가가 개인인 생산한 전력만큼 전력을 적게 생산해도 되기 때문이다. 특히 실시간 전력 가격이 도입된다면 전력관리의 효율성은 더욱더 증가된다.

개인 간 전력거래 활성화는 2가지 제약사항으로 인해서 어려움을 겪고 있다. 첫째, 전력거래의 보안 취약성이다. 전력거래는 사물인터넷을 기반으로 하고 있기 때문에 해킹의 위협을 받을 것이다. 둘째, 거래 과정의 비효율성이다. 전력거래를 위해서는 거래소, 은행 등 여러 중개기관을 거쳐야 한다. 이는 거래 복잡성을 일으킬 뿐만 아니라 전력거래 판매자들 사이 이득을 감소시킨다. 중개기관들은 중개한 대가로 수수료를 요구하기 때문이다.

이러한 제약사항을 블록체인이 해결해줄 수 있다. 거래 위변조를 방지해주고 스마트 컨트랙트의 경우 중개기관 없이 거래를 가능케 한다. 2016년 4월 미국 브루클린 지역에서는 '트랜젝티브그리드(TransactiveGrid)'와 'LO3 에너지'가 합작해서 태양광으로 생산한 전력을 개인 간에 사고 팔 수 있게 했다. 독일의 전력생산회사인 RWE는 블록체인으로 전기차가 전력을 거래할 수 있게 구현했다. RWE는 슬록(Slock)과 함께 전기자동차 충전거래 시스템을 개발 중에 있다고 밝혔다. 기존에는 머문 시간만큼 요금이 책정 돼 불합리했다. RWE가 개발하고 있는 방식은 충전한 전기량만큼 요금이 부과돼, 좀 더 합리적이다. 사전에 충전할 양과 금액을 스마트계약으로 입력하게 함으로써 이러한 서비스가 가능해지는 것이다.

전자 문서 관리

- **비용절감/안전성/투명성/편의성**

전자문서는 보통 중앙서버에 기록한다. 이는 문서가 위변조 될 위험을 발생 하게 한다. 기관의 악의적인 행동 혹은 해커의 사이버 공격으로 문서를 위변조할 수 있기 때문이다. 그뿐만 아니라 운용비용도 많이 든다. 중앙서버에 있는 전자문서를 안전하게 보호하기 위해서는 여러 보안 장비가 구축되어야 하는데 이는 장비구매와 유지하는 데에 비용을 소모하게 한다. 아울러 문서를 저장하는 서버 또한 관리해야 하므로. 서버 유지비용도 발생한다.

블록체인은 이러한 기존 전자 문서 관리의 문제점을 해결해줄 수 있다. 중앙시스템의 문서 관리 비용을 줄여주고 문서 내용 위변조 위협으로부터 안전하게 보호해준다. 전자문서 관리 사례를 통해 전자문서 관리 이점을 살펴보면

- 전자문서 관리비를 절감: 국내 통신기업인 kt는 전자 서명 관리 시스 템인 'ESC (Electronic data & Signature Capture)'를 개발했다고 밝혔다. 그리고 BC카드에 이를 적용했다. ESC는 전자 서명을 블록체인으로 관리하는 기술이다. 2017년 3월 전자 서명을 ESC로 시범 적용해 보았다. 적용결과 기존 전자 서명 관리 시스템보다 파일 처리 시간을 최대 70% 까지 서버 사용 용량은 80%까지 줄일 수 있었다고 한다. 이에 따라 BC카드는 ESC 적용으로 관리비용을 절감시킬 수 있을 기대된다.
- 안전한 문서 보관: 블록체인에서 모든 문서는 중앙에서 관리되지 않고 분산되어서 반영구적으로 보관된다. 블록체인에 저장한 문서는 위변조될 위험이 거의 없다고 볼 수 있다. 에스토니아는 전자문서에 고유한 서명 값을 발급해서 위변조를 방지한다. 이러한 서명 값을'KSI (Keyless Signature Infrastructure)'라도 부르는데, KSI를 블록체인에 안전하게 저장한다. 따라서 KSI가 조작될 가능성은 실질적으로 불가능하다. 카카오도 블록체인의 이러한 안전성을 착안해서 블록체인 기반의 문서관리시스템을 만들 계획이다.
- 정부가 문서를 가지고 비리를 저지를 수 없게 함: 위변조할 수 없고 중앙에서 관리되지 않기 때문이다.
- 문서의 공유가 용이: 블록체인은 서비스 당사자 모두 정보를 가지고 있다. 중앙방식처럼 정보를 주고받을 필요가 없다. 그래서 문서정보 공유에 드는 시간과 비용을 절감할 수 있다. 스웨덴의 토지대장 관리는 블록체인에 토지대장 관리를 넣으면 정보를 공유하기 때문에 심사 기간을 단축시킬 수 있는 이점이 있다.

음반 산업

수익성과 저작권 보호

음반 산업의 구조를 살펴보면 음악 생산자인 가수가 있고 이를 유통하는 유통회사 그리고 이를 소비하는 소비자가 있다. 음반 산업의 지배 구조를 살펴보면 유통회사가 시장을 거의 독점하고 있다. 그래서 유통회사는 수수료를 높게 책정해서 높은 수익을 올리는 반면에 음반사는 제 값을 제대로 받지 못하고 있다.

이러한 문제점을 블록체인을 활용하면 풀 수 있다. 스마트 컨트랙을 이용하면 개인 간 음반거래가 가능하다. 음반을 스마트 컨트랙에 등록하고 음반에 특정코드를 삽입한다. 특정코드는 스마트 컨트랙에서 만들어진 것으로, 특정 가상화폐를 지불해야지 풀리도록 되어 있다. 참고로 이러한 가상화폐는 음원 생산에 기여한 관계자들에게 일정 수익률로 배분할 수 있게 설정해서 받을 수 있다. 예를 들어 비트코인 기반으로 음원을 암호화 했다면 비트코인을 지불해야지 음반의 암호화가 풀린다. 비트코인만 이용할 줄 알면 유통사를 거치지 않고 음원을 쉽게 거래할 수 있다.

잠깐!

스마트 컨트랙
블록체인 기반으로 금융거래, 부동산 계약, 공증 등 다양한 형태의 계약을 체결하고 이행하는 것을 말한다. 스마트 컨트랙은 신뢰할만한 제3자의 역할을 프로그램이 대신한다. 특히 블록체인은 중앙집권화 된 기관이 없이도 블록체인 참여자를 통해 계약의 신뢰성을 확보하고 거래를 진행한다. 비트코인 거래 자체도 스마트 계약의 사례라고 할 수 있다. 앞서 용어설명에서 언급했던 '에스크로'는 상거래에서 판매자와 구매자 사이를 신뢰할 수 있는 제3자가 중계하는 서비스로 스마트 컨트랙 유형으로 볼 수 있다.

실제로 2015년 10월 미국 유명 가수인 이모겐 힙(Imogen Heap)은 블록체인을 기반으로 음원을 발매한 적이 있다. 이모겐은 개발자의 도움을 빌려서 블록체인으로 음원을 발매하도록 계획한 것이다. 블록체인으로 음원을 발매하면 생산자는 중개비용 감소로 더 높은 이윤을 창출할 수 있다. 물론 줄인 중개비용에서 일정 이상을 음원 판매 가격에도 반영한다면 소비자는 더 저렴한 가격으로 음원을 즐길 수 있다.

이외에도 저작권 침해를 예방할 수 있는 효과도 기대할 수 있다. 음원 자체를 블록체인으로 발매하면 음원을 암호화하기 때문에 무단 배포를 예방할 수 있다. 침해가 되더라도, 블록체인에 이력이 남기 때문에 사후 대응도 가능하다. 미국 버클리 음악 대학교는 블록체인을 적용해서 음반 저작권료 지급 시스템을 개발할 계획이라고 밝혔다.

기부 산업

- **신뢰성 보장**
  기부자들은 본인의 돈이 어디에 사용되는지 알 수가 없어서 기부 단체들을 신뢰하지 못한 경우가 많다. 이에 따라 기부금액에 대한 정보를 블록체인 방식으로 제공하는 기관들도 늘어나고 있다. 기부 산업의 사업 관점은 바로 '신뢰성'이다. 신뢰성을 제공해서 기부자들이 믿고 돈을 기부할 수 있게 하는 것이다. 헬프빗(HELPERBIT)은 기부 금액을 블록체인 방식으로 도입해서 기부자들이 쉽게 기부 금액 사용내역을 조회할 수 있게 했다. 이외에 엘리스(Alice), 기브트랙(Givetrack)도 블록체인을 이용해서 기부자에게 기부금 사용내역을 공개하고 있다.

감별 산업

신뢰성 보장

블록체인을 감별 산업에도 적용할 수 있는데 가장 큰 시장은 '다이아몬드'이다. 다이아몬드는 고가의 제품이기 때문에 감별이 매우 중요하기 때문에 감별사가 다이아몬드 진위여부를 판별하는 경우가 많다. 그런데 이를 블록체인으로 다이아몬드의 진위여부를 증명할 수 있다.

에버레져(Everledger)는 다이아몬드의 이력을 블록체인으로 기록해서 다이아몬드 진위여부를 판별하게 한다. 다이아몬드는 고가이기 때문에 참여자 또한 신뢰할 만한 기관으로 구성돼 있다. 보험사에서부터 시작해서 법률기관까지 포함돼 있다.

다이아몬드 뿐만 아니라 음식도 블록체인으로 감별할 수 있다. 프로베넌스(Provenance)는 음식의 진위여부를 블록체인으로 감별할 수 있는 서비스를 제공하고 있다. 프로베넌스는 음식의 유통과정을 블록체인으로 기록함으로서 중간에 식품 조작을 막는다. 현재 200여 곳 이 상의 유통업체가 프로베넌스의 서비스를 이용하고 있다.

전자투표

안전성과 투명성 보장

공공 분야에서 블록체인이 가장 큰 빛을 바라는 곳은 전자투표이다. 투표조작은 민주주의 어느 국가든 우려를 하고 있는 문제이다. 투표조작을 우려하는 것은 국내나 해외도 마찬가지이다. 미국은 작년 대선 때 에 투표조작 의혹을 제기 했었다. 위스콘신, 미시간, 펜실베이니아 주에서 투표 조작의혹을 제기한 것이다. 프랑스는 전자투표를 진행하는 국가인데, 올해 해킹으로 투표가 조작될까봐 전자에서 종이로 바꿨다.

이러한 투표조작 문제는 전자투표 시스템에 블록체인을 활용하면 해결이 가능하다. 블록체인 데이터는 공유되기 때문에 시민들이 감시할 수 있다. 아울러 분산형태로 원장에 저장되기 때문에 투표조작 공격에도 안전하다. 이러한 이유로 블록체인을 전자투표에 적용하려는 움직임이 늘고 있다. 에스토니아의 의회선거, 덴마크 당 내부 투표, 미국 대선후보 선정 등 여러 국가에서 블록체인을 투표에 적용하고 있다. 국내도 블록체인을 투표에 활용한 사례가 있다. 2017년 2월 23일 경기도는 주민제안 공모 사업인 '따복 공동체'에 최초로 블록체인을 적용해서 투표를 했다.

03. 블록체인과 사이버 보안

1 비트코인 가격은 2011년 상반기만 해도 1달러를 겨우 넘기는 수준이었다. 그러나 2017년 11월 8일 기준으로 1 비트코인 가격은 무려 7,400 달러에 이르고 있다. 6년 만에 비트코인 가격이 7,400배나 오른 것이다. 그래서 비트코인은 해커들의 해킹 대상이 되어 왔다. 가장 대표적인 사례가 '마운트 곡스' 파산 사건으로 마운트 곡스는 비트코인 거래와 지갑을 운영하는 곳으로, 2014년 전까지 세계에서 가장 큰 비트코인 거래소였다. 비트코인의 가장 큰 거래소였던 마운트 곡스가 2014년 2월 28일에 갑자기 파산을 신청하게 된다. 보유 중인 85만 개의 비트코인이 도난당했기 때문이다. 당시 가치로는 4억 5천만 달러(한 화로 약 5천 3백억 원) 이나 되는 금액이 도난당한 것이다. 올해 11월 기준으로 가치를 환산하면 무려 약 63억 달러(약 7조 원)이나 된다. 국내에서도 여러 차례 발생했었다. 올해 4월 국내 비트코인 거래소 '야피 존'은 3,831비트코인을 도난당했다. 해킹 당시 기준으로 피해액은 55억 원이었고, 11월 기준으로는 약 315억 원이나 된다.

물론 마운트 곡스와 야피존 해킹 피해 원인은 바로 비트코인 소유주를 인증 하는 '개인키'가 도난당했기 때문이다. 지금까지 알려진 비트코인 해킹 사건 모두 개인키 도난으로 발생했다. 블록체인의 장점 중 하나를 해킹에 대한 보안성으로 꼽았다. 블록체인 피해는 있는데 왜 안전한 것일까? 이 물음에 대한 답을 학습하기로 한다.

블록체인의 보안성 분석

비트코인이 블록체인을 가장 잘 대표하고 있고 비트코인에 대한 해킹사례가 많아서 분석이 용이하고 일반사람들에게 비트코인에 대한 인식이 높기 때문에 블록체인 보안성 분석의 대상을 비트코인로 정하여 분석한다. 보안 수준은 기밀성, 무결성, 가용성, 익명성, 인증, 부인방지 분야에 대하여 분석한다.

- 기밀성

블록체인 기밀성 수준은 높다. 블록체인은 공개 키 암호화를 이용하고 있다. 블록체인의 모든 중요 정보는 SHA 256으로 암호화된다. 그리고 다시 한번 BASE58Check에서 문자로 변환 시킨다. 이를 풀기위해서는 개인키가 있어야 한다. 개인키가 없다면, 역순으로 해킹하기란 무척 어렵다. SHA 256 경우만 하더라도, 이론상 2의 256승만큼 시도를 해야 하기 때문이다.

잠깐!

SHA-256(Secured Hash Algorithm-256)
어떠한 입력 데이터를 입력하면 동일한 길이의 랜덤 숫자로 변환시키는 암호 알고리즘. SHA-256은 임의의 데이터를 입력하면 256비트(32바이트)의 값을 생성하는데 이것은 데이터에 대한 지문 역할을 함.
BASE58Check: Base58은 binary data를 text로 변경해 주는 encoding 기법 중의 하나

- 무결성

무결성에서 측정해야 항목은 두 가지이다. 정보를 송수신할 때의 무결성 여부와 보관하고 있는 정보의 무결성 여부이다. 전자의 경우는 공개키 암 호화로 안전하다. 해커가 정보를 위변조하기 위해서는 '개인키'가 있어야 한다. 없을 시에는 SHA 256으로 암호화 된 값을 해킹해야 하는데, 앞서 설명했듯이 어렵다. 그래서 정보를 송수신 할 때의 무결성 수준은 높다. 두 번째로 정보 기록의 무결성이다. 블록체인의 최대 장점은 기록된 정보의 높은 무결성 이다. 블록체인 매우 높은 수준의 정보 무결성을 제공한다. 이는 블록체인이 가진 가장 큰 장점이자, 정부가 블록체인에 주목케 하는 이유라고 볼 수 있다. 블록체인의 정보 무결성이 높은 이유는 '분산형 원장'의 원리로 정보를 기록하기 때문이다. 블록체인에서 발생한 모든 정보는 모든 노드에 기록된다. 그리고 노드에서는 저장한 데이터는 위변조 되었는지 확인하기 위해서 끊임없이 대조를 한다. 이러한 과정에서 저장한 데이터가 노드 사이에서 내용이 불일치가 발생할 경우 다수 노드가 기록한 데이터 내용에 따라서 불일치를 수정한다. 이는 해커가 전체 노드 중에서 과반수 계정을 해킹해야 하는 것을 의미하고, 거대 IT 기업만이 보유할 수 있는 슈퍼컴퓨터로 동시에 노드의 계정을 해킹해야 함을 의미 한다. 이론상으로 가능하나 현실적으로 매우 어렵다.

- 가용성

비트코인의 블록체인은 '서비스 분산 공격'처럼 가용성을 위배하는 공격을 당할 일이 없다. 개인이 이러한 공격을 당해 피해를 입을 수 있겠지만 비트코인 블록체인 시스템 자체가 이런 공격에 당할 일이 없다. 중앙 시스템이 없기 때문이다. 그럼에도 불구하고 비트코인이 서비스 분산 공격 피해를 입었다는 기사를 접하게 된다. 이는 오해의 소지가 있는 기사이다. 기사를 살펴보면 비트코인 자체가 서비스 분산 공격을 당한 것이 아니라, 비트코인의 거래를 담당하는 거래소가 서비스 분산 공격에 당한 것임을 알 수 있다. 아울러 개인도 당할 수 있다. 개인 컴퓨터가 서비스 분산 공격을 당해서 전원을 켤수 없을 수도 있다.

- 익명성

비트코인의 익명성 수준은 매우 높다. 비트코인 활용 시에 개인정보과 관련한 어떤 정보도 요구하지 않기 때문이다. 비트코인 이용 시에 주민번호, 전화번호 등 개인과 관련한 정보를 전혀 묻지 않는다. 심지어는 딥넷(Deep Net) 처럼 IP 주소도 기록되지 않는다. 이러한 이유로 해커들은 다크넷(Darknet)에서 거래 시에 비트코인을 이용한다. 개인정보가 전혀 남지 않기 때문이다. 최근 랜섬웨어의 금전 댓가로 비트코인을 많이 이용 하는 경우가 있는데, 사이버 수사대의 추적을 피하기 위해서이다. 비트코인은 가상화폐이기 때문에, 정부통제가 거의 불가능하다. 이를 악용해서 불법자금 뿐만 아니라 세금을 피하기 위한 용도로도 활용 되고 있다. 비트코인의 높은 익명성으로 인해서 오히려 지하경제에서 활용 되는 부작용을 낳았다.

- 인증

거래를 하기 위해서는 개인키가 있어야 한다. 개인키는 비트코인 소유를 인증하는 수단이기 때문이다. 그래서 개인키를 도난당했다는 의미는 개인키에서 보유하고 있는 비트코인을 잃어버린 것과 같다. 비유하면 개인키는 지갑인 셈이다. 비트코인 보안 취약점은 바로 '개인키'이다. 비트코인에서는 별도로 개인키 관리를 위해서 특별한 보안 솔루션을 제공하지 않는다. 개인이 관리해야 한다. 이는 비트코인이 도난당하는 불상사를 발생하게 한다. 앞서 언급한 야피존을 비롯해서 여러 비트코인 해킹 사례는 개인키 도난과 관련 되어 있는 것이다. 비트코인 시스템의 인증 자체는 공개키 암호화를 사용하기 때문에 높다. 공개키로 암호화하고 개인키로 인증하기 때문이다. 그러나 비트코인 개인키가 도난당할 수 있는 위험 이 있기 때문에 인증의 보안 요구사항은 낮다.

- 부인방지

블록체인은 분산형 원장 방식으로 기록하기 때문에 서비스를 제공받은 사람이 서비스 제공 사실을 부인할 수 없다. A가 B에게 비트코인을 송금한다고 가정하자. B는 A에게 B의 개인키로 변형한 공개키를 보낼 것이다. A는 B의 공개키로 비트코인을 입금한다. 그러면 B는 본인의 개인키로 인증해서 비트코인을 받는다. 이때 B가 비트코인을 받았다는 사실이 A에게 전송된다. A 뿐만이 아니다. 비트코인의 모든 노드로 전송 된다. 비트코인 참여자 모두가 증인인 셈이다. 그렇기 때문에 비트코인을 받지 않았다고 부인하기가 어렵다. 부인내용도 조작할 수 없다. 앞서 언급했듯이 과반수 사용자 계정을 해킹하고 슈퍼컴퓨터를 이용해 기록 정보를 위변조 해야 한다. 이는 언론에 공개된 사실을 지우려고 노력하는 것과 같다고 보면 된다. 정리하면 블록체인 부인방지 수준은 매우 높다.

블록체인의 보안 취약점은 '개인키 관리'에 있다. 비트코인 개인키 관리에 대해서는 피해 예방과 피해 최소화로 나눠서 대응해야 한다. 피해 예방은 말 그대로 비트코인 도난을 예방하는 것이다. 개인이 예방할 수 있는 방법은 크게 없다. 단지 개인키를 안전한 외장하드에 담아야 한다. 그리고 함부로 외부에서 외장하드를 다른 기기와 연결해서는 안 된다는 것이다. 기기가 악성코드에 감염돼 있을 수도 있기 때문이다. 아울러 본인 기기와 연결할 때에도 그전에 먼저 백신을 실행시켜서 악성감염 여부를 확인하는 것이 좋다.

- **4차산업 혁명의 엔진 'ICBM'의 한계점과 블록체인 대두**

ICBM이라는 엔진으로 구동되는 4차 산업혁명은 ICBM 플랫폼이 가지는 다음의 4가지 한계점을 해결하지 않고서는 사상누각에 불과할 수 있다.

- 보안 취약성: 4차 산업혁명은 '초 연결성'의 특징을 지니지만 이러한 연결이 사이버 보안에 취약한 센서 기술인 사물인터넷을 기반으로 하고 있다는데 문제가 있다. 센서는 크기가 작고 컴퓨터와 스마트폰 보다 하드웨어 성능이 훨씬 낮아 센서에 보안 솔루션을 적용 하는 데에 한계점이 있기 때문이다. 2016년 10월 미국에서는 '미라이(Mirai)'라는 악성코드로 인한 디도스 공격으로 아마존, 트위터, 넷플릿스, 뉴욕타임즈 등 미국의 주요 기관들의 웹 사이트가 피해를 당했다. 다른 디도스 공격과 별반 다른 게 없지만 좀비 기기 대상이 일반 컴퓨터가 아닌, 사물인터넷 기기를 이용했다는 점에서 사이버 보안 업계에 큰 충격을 줬다. 더 놀라운 사실은 정교한 공격기법 없이 단순히 초보적인 방식으로 10만 대가 넘는 사물인터넷 기기를 감염시켰다는 것이다. 이는 사물인터넷이 보안에 얼마나 취약한지를 보여준다.

- 사생활 침해: 모든 정보들이 클라우드에 관리가 되는 것은 사용자에게 편리함을 준다. 사용자 기기에서는 분석할 수 없는 정보들을 빅데이터 분석해서 새로운 서비스를 제공하지만 다른 한편으로는'사생활 침해'라는 문제를 야기한다. 현재 개인정보들은 허락 없이 마케팅 용도로 활용되고 있다. 거의 모든 시스템이 클라우드 방식으로 운영됨에 따라 사생활 침해 문제는 앞으로 더욱더 심각해질 것으로 보인다.

- 중앙화: ICBM 플랫폼은 모든 정보를 중앙 센터 클라우드에 모아서 처리한다. 이는 정보 중앙화와 관련한 문제가 발생할 수 있다. 정보가 중앙에 모이는 것 자체에는 큰 문제는 없지만 이를 악용할 때 발생할 수 있다. 전자투표를 예를 들면, 투표자들이 입력한 투표내용은 개인에게 저장되는 것이 아니라 중앙 데이터베이스에 기록된다. 본인이 투표한 것에 대해서는 알고 있지만 다른 사람이 투표한 내용은 알 수 없다. 결국 정보를 가지고 있는 중앙기관이 투표결과를 왜곡할 수도 있다.

- 클라우드 수용 용량 초과: 거의 모든 기기들이 네트워크에 연결되고 있다. 사물인터넷이 보편화됨에 따라 사물인터넷 기기는 200억 개보다 더 많은 숫자로 늘어날 것으로 보인다. 중앙에서만 무수히 많아진 사물인터넷 기기를 관리하는 것은 비용 측면에서 무리가 있다.

4가지 문제점은 4차 산업혁명이 가질 수밖에 없는 한계점으로 인식되어 왔다. 그런데 이러한 한계점을 해결할 기술이 등장했다. 바로 '블록체인'이다. ICBM 플랫폼은 '중앙형'이라면, 블록체인은 '분산형'이라는 특성을 가지고 있다. 따라서 블록체인은 ICBM 플랫폼의 한계점을 보완해줄 것으로 전망되어 전 세계로부터 주목을 받고 있다. 그렇다면 블록체인의 분산형 특성이 4차 산업혁명에서 제기되는 한계점을 어떻게 해결할 수 있는 것일까?

- 사이버 공격에 견고: 블록체인은 분산형 원장이기 때문에 블록체인에 기록하고 있는 정보를 위변조시키는 것을 거의 불가능하게 한다. 특히 비트코인의 거래는 공개키 암호화를 사용하고 있기 때문에 비트코인의 경우 '중간자 공격'이 어렵다. 비트코인 해킹이 있었는데, 이는 개인의 개인키를 제대로 관리하지 못해서 발생한 사건이다. 따라서 개인키만 도난당하지 않으면, 안전하다고 봐도 무방하다.

잠깐!

중간자 공격(man in the middle attack)
통신하고 있는 두 당사자 사이에 끼어들어 당사자들이 교환하는 공개정보를 자기 것과 바꾸어버림으로써 들키지 않고 도청을 하거나 통신내용을 바꾸는 수법

- 사생활 침해의 우려가 없다: 블록체인 구조에서는 중앙 관리자가 없고 데이터는 익명으로 모든 기기에 기록된다. 주민번호, 전화번호, IP 등의 주소가 전혀 기록되지 않는다. 그러므로 블록체인에서 발생한 개인 관련 정보는 안전하게 보관될 뿐만 아니라, 중앙관리자가 기관의 이익을 목적으로 개인정보를 침해할 일도 없다.

- 민주적이다: 블록체인 발생한 거의 모든 거래 내역은 공유된다. 사물인터넷에 블록체인을 적용한 IBM은 블록체인 시대로 인해서‘ 기기 민주화 (Device Democracy)’라고 표현했다. 기존의 중앙 서버 방식은 중앙에서 모든 것을 운영되게 했지만 블록체인은 분산된 기기에 의해서 자동으로 운영되기 때문이다.

- 중앙센터의 관리비 부담이 없다: 블록체인에서는 중앙 관리자가 없다. 그러므로 중앙센터가 없고, 노드에서 모든 것들이 처리된다. ICBM 방식의 경우 사물인터넷으로 증가하는 기기들을 관리하는 데에 부담이 많았다. 그러나 블록체인은 노드가 늘어나더라도 부담이 분산되는 것이다.

- 신뢰성이 있다: 모든 정보가 공유되고 있기 때문에 조작의 위험이 없다. 이는 블록체인 기반의 서비스에 신뢰성을 제공한다.

블록체인이 ICBM 보다 우월한 기술이기보다는 서로 상반되는 기술이기 때문에 블록체인이 가지고 있는 특성은 ICBM이 가지고 있는 한계점을 극복해 줄 것으로 보인다. , 블록체인에 없는 특성이 ICBM에는 있다. 예를 들어 고도의 분석기술을 개인 저 사양 단말기에도 제공해줄 수 있는데, 중앙센터의 클라우드에서 처리하기 때문에 가능하다. 반면에 블록체인은 불가능하다. 중앙에서 대신 처리할 수 있는 클라우드 서버가 없기 때문이다.