이더리움 개론 (Ethereum Introduction)

한승환 (필명: 어른아이)

차세대 신기술로는 여러가지가 각광을 받고 있지만, 그 중 디지털 분야에서 가장 혁명적인 기술로 평가받는 기술은 블록체인에 기반한 이더리움 플랫폼이라고 할 수 있다.

이더리움은 '월드테크놀로지(The WTN) IT S/W'부문에서 경쟁작인 마크 저커버그의 페이스북을 제치고 수상을 하게 된다. 또한 웹 3.0과 사물인터넷(IoT) 시대에 주요하게 사용되고 응용될 기술로 주목받고 있다.

이더리움을 한 문장으로 정의하자면:
"**블록체인을 활용한 모든 것을 프로그래밍할 수 있는 플랫폼**"이라고 할 수 있다.

아래 몇 가지를 검토하면서 이더리움(Ethereum)이 무엇인지 알아보겠다.
-깊게 들어가면 끝도 없이 어려운 내용일 수 있지만, 핵심을 다루면서도 최대한 이해가 쉬울 수 있는 방향으로 서술하였다. 블록체인이나 이더리움의 개념이 생소한 사용자들에게 기초가 될 수 있도록 의도하였다.

목차

---

1. 블록체인

블록체인은 중앙서버 없이 'P2P로 구현되는 비가역적 공유 데이터베이스'라고 정의할 수 있다.

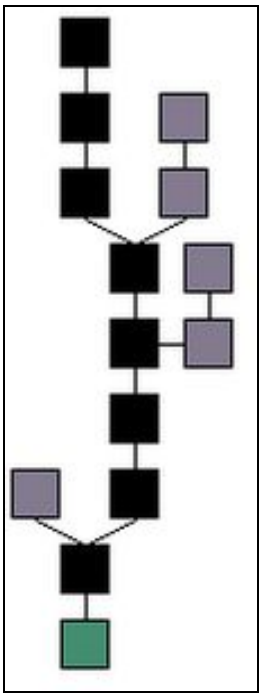
P2P방식으로 이루어진 네트워크에서 참여자(Node, Client)들은 데이터를 담은 블록을 생성하고 검증을 한다.

각 참여자들은 일정한 규칙에 따라 데이터를 담은 블록을 경쟁을 통해 생성하게 되며, 이러한 블록은 일정 컴퓨팅 파워가 투입된 이후에는 비가역적(Irreversibility)이 된다(=되돌릴 수 없다).

이전의 디지털 세계에서는 기존의 데이터를 조작, 삭제, 취소하는 것이 매우 쉬웠기 때문에 특정한 디지털 코드가 가치를 지니게 되기는 쉽지 않았으며, 디지털 코드를 심지어 화폐로 사용하는 것은 불가능하였다. 그렇게 때문에, 중앙에서 통제하는 디지털 화폐나 재화(은행전산망 안의 계좌잔고, 게임머니, 웹하드 포인트, 시리얼 키를 가진 소프트웨어 등)에 절대적 통제권을 행사하여 외부에서 조작할 수 없도록 보안을 유지해야 했다. 물론 그러한 보안이 완전할 수 없기 때문에 해킹사고는 빈번히 일어나 왔고, 중앙권력 자체가 해당 재화를 직접 조작하고 유용하여 부당학 이익을 취득하는 사기도 매일의 일상이다.

그러나 블록체인을 통해 중앙권력없이 순수하게 사용자들로만 이루어진, 그리고 조작이나 통제가 불가능한 시스템이 갖추어지게 되었다.

(오른쪽은 블록체인의 도식이다)



<그림 1(출처)>

그림설명
각 블록이 이전블록을 근거로 생성(아래에서 위방향)되고 있다.

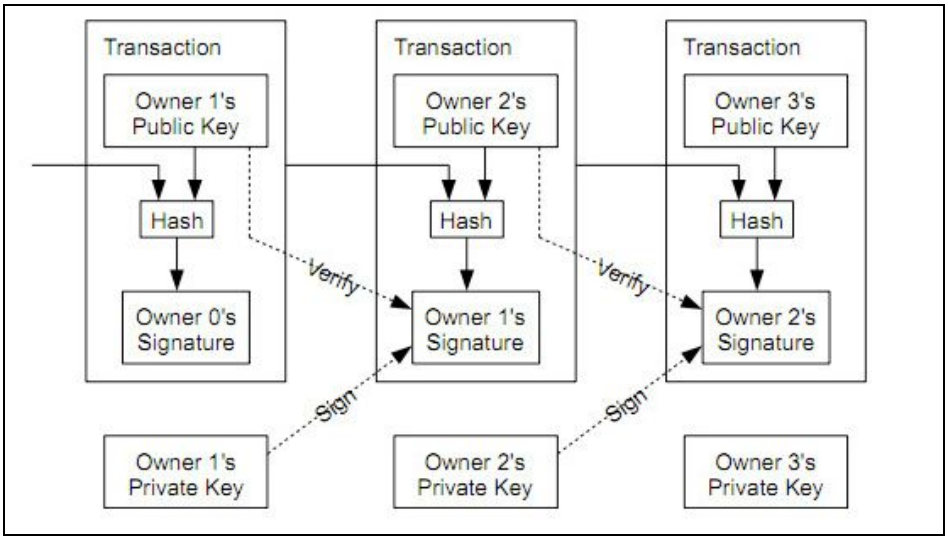
녹색은 최초의 블록(탄생블록: Genesis block)이며, 이 녹색블록 없이 그 위의 블록을 만드는 것은 불가능하다. 따라서 각 블록이 이전 블록의 정보를 가지고 있고 그것이 모여 체인을 이룬다(블록체인).

검은색은 해시파워(CPU power)를 통한 경쟁에서 승리하여 블록생성에 성공하고, 실제 블록체인의 일부가 된 블록들이다. 따라서 해당 블록안의 데이터는 해당 네트워크에서 '공유지식'이 된다.

보라색은 경쟁에서 실패하여, 블록체인의 일부가 되지 못한, 즉 네트워크에 공유되지 못하며 인정받지 못하는 블록이다(따라서 해당 블록안의 데이터도 블록체인의 일부가 되지 못한다). 이러한 블록은 폐기된다.

탄생블록부터 경쟁에서 이긴 블록들어 이루어진 체인을 '주체인(Main chain)'이라 칭하며, 이곳에 들지 못한 블록을 '탈락블록(Orphan/ Stale/ Invalid Block)'이라 칭한다. 주체인 상의 블록에 포함되어 있는 데이터 내역만이 유효한 것으로 인정받게 된다.

<그림2(출처)>



위의 '그림1'이 블록들의 체인이라면, '그림2'는 블록 안의 데이터들의 체인이라고 볼 수 있다. 각 블록안을 들여다 본 모습이다. 각 블록 안에는 데이터의 집합이 있는데, 각 데이터는 위와 같이 전자서명을 통해 연결되어 있다. 이전 데이터가 없이는 이후의 데이터가 나올 수 없다. 따라서 각 데이터는 모두 연결되어 있고 서로의 유효성을 증명하는 역할을 한다. 이렇게 기존 내역을 근거로 불일치하는 내역이 있을 시 오류처리된다.

비트코인의 경우, 이러한 블록체인을 통해 '비트코인'이라는 가상화폐를 거래하게 된다. 이전의 거래(입금)내역이 없다면 당연히 출금할 수 없다. 입금 받은 금액 이내에서 이체가 되며 이체한 금액은 다른 사용자의 지갑주소로 들어가 해당 사용자가 또 다시 이체할 수 있게 된다.

블록체인은 디지털 화폐가 복제될 수 없고, 거래내역이 변조될 수 없으며, 완료된 거래가 취소될 수 없도록 비가역성을 보장해주는 역할을 하게 된다. 이를 통해 중앙서버나 통제기관 없이 네트워크 안의 사용자들만으로 자유로운 화폐거래가 가능하게 되었다.

1-1. 작업증명(Proof-of-Work)과 해시알고리즘(Hash Algorithm)

1) 각 네트워크의 작업증명(Proof-of-Work)처리에 참여하는 노드(Node)는 자신이 네트워크 상으로 전달받은 거래내역들을 자신의 '거래내역저장고(Transaction Pool)'에 보관해둔다.

2) 일정한 해시알고리즘을 통해 특정한 난이도의 해시값을 생성해내는 작업을 한다. 이 중 '목표값(Target Hash Value)'를 찾아내는 사람은 블록 생성권한을 획득하게 된다.

3) 목표값을 찾기 위해서는 미리 설정된 '해시 알고리즘'(특정한 입력 값을 동일한 길이의 무작위 해시값으로 변환해내는 공식)을 적용해서 작업을 해야하는데, 비트코인의 경우 SHA-256이라는 해시알고리즘을 사용한다.

4) 시스템에 의해 설정된 목표값을 빨리 찾아내어야 경쟁에서 이기고 자신이 생성한 블록을 전체에 먼저 '공표(Public Announcement)'할 수 있게 된다. 다른 노드들도 동일한 작업에 참여하고 있기 때문에 속도가 매우 중요하다. 뒤 늦게 하는 '공표'는 주체인(Main Chain)에 산입되기가 '거의 불가능'하므로 의미가 없다.

5) 이러한 속도를 늘리기 위해서는 더 많은 컴퓨터 자원을 사용하는 수 밖에 없다.

6) 이러한 해시알고리즘 사용의 목적은 해싱작업을 통해 '경쟁'을 하기 위해서이다. 그래서 더 높은 난이도의 목표값을 더 빨리 찾는 사람이 블록생성을 하게 만들고 결국 블록생성/조작을 위해서는 그만큼 비용(컴퓨팅기기, 전기세, 관리비 등)을 들게 만드는 것이 궁극의 목적이다(즉 권한을 획득하고 싶다면 돈을 내라는 것, 순수하게 돈으로 해킹이 가능한 시스템이다). 따라서 보안성이 증명된 알고리즘이라면, 어떠한 알고리즘을 사용하든 크게 상관이 없다.

2. 암호화화폐의 발전과정

1) 비트코인(Bitcoin)
완전한 의미의 블록체인을 처음으로 활용한 예는 비트코인이다.
비트코인은 디지털 화폐인 '비트코인'을 거래할 수 있도록 해주는 시스템 프로토콜/프로그램이다. 비트코인의 거래내역이 담긴 블록을 생성하는 방법은 CPU파워를 투입해서 특정 해시값을 찾아내는 경쟁을 하는 것인데, 당연히 CPU파워를 더 많이 투입한 사람이 더 많은 블록을 생성할 수 있게 된다.

2) 네임코인(Name Coin)
비트코인은 화폐로써 교환의 매개역할만을 수행한다. 그러나 네임코인은 한단계 더 나아가서, 각 네임코인을 신규도메인을 만들 수 있는 권리를 대표하는 '토큰(Token)'의 역할도 할 수 있도록 하였다. 네임코인은 비트코인처럼 화폐로 거래될 수 있으며, 탈중앙화된 도메인을 등록할 수 있는 토큰의 역할도 하는 이중활용을 가능하게 하였다.

도메인은 '닷빗(.bit)'을 사용한다. 해당 도메인으로 개설된 싸이트들도 존재한다(하지만 현재는 인기가 시들어짐에 따라 대부분 서비스도 종료되었다).

3) 프라임코인(Prime Coin)
현대 시대에서 디지털 상의 보안성은 대부분 소수(Prime Numbers)의 비대칭성(Asymmetric Property)을 활용하여 이루어진다.

따라서 소수를 찾는 작업이 매우 중요한데, 프라임코인은 그 중 쌍둥이 소수(Twin prime numbers)의 무한성을 증명하는 알고리즘(두 개 이상의 체인을 사용하는 Cunningham/TWN)을 사용하여, 컴퓨팅파워를 활용한다.

4) 컬러드코인(Colored Coin) - 관련동영상
결국 여기까지 왔다. "왜 굳이 비트코인은 비트코인으로만 사용해야할까? 비트코인에 '대표성'을 입히자"라는 생각에서 출발한 코인(엄밀히 말하면 비트코인 네크워크에 기생하는 보조체인)이다.

각 코인에 색을 입혀서(물론 상징적인 의미로), 녹색 비트코인은 내 자동차의 소유권을, 파란색 비트코인은 내 집의 소유권을 대표하는 것으로 하고, 각 코인을 가진 사람에게 해당 재산의 소유권을 인정해주기로 하는 것이다.

따라서 1 비트코인이라는 상징성은 사라지고, 해당 비트코인이 대표하는 자산인 자동차나 부동산으로 취급되어 거래가 될 수 있다. 다만, 개념적으로는 혁신적이었으나 현실적인 법리문제 등이 대두되면서 실현가능성 여부에 대해서는 비판을 받았다.

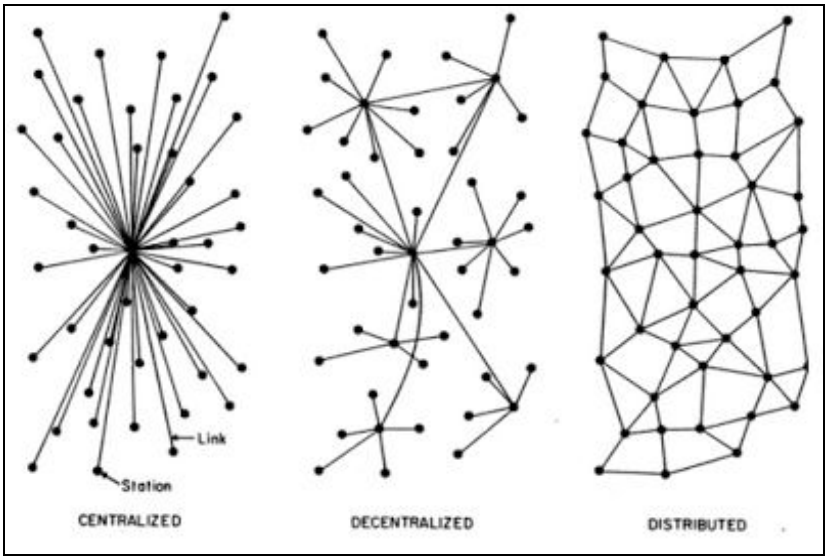
5) 이더리움(Ethereum) - 국내싸이트 이더리움코리아
'블록체인2.0' 시대를 표방하며 나온 혁신적인 개념의 기술이라고 볼 수 있다.
비트코인이 화폐이고,
네임코인이 화폐와 토큰의 역할을 하였으며,
프라임코인이 컴퓨팅 파워를 이중적으로 활용하였고,
컬러드코인은 화폐가 특정 자산을 대표할 수 있도록 하였다면,

이더리움은 블록체인을 하나의 데이터베이스로 보고, 모든 자산을 올릴 수 있고 각 자산이 구동하거나 거래되는 방식까지 직접 프로그래밍할 수 있는 하나의 '오픈플랫폼(Open Platform)'으로써 설계되었다. - (플랫폼 경제학 참조)

이더리움 상에서는 비트코인/네임코인/프라임코인/컬러드 코인을 모두 설계할 수 있을 뿐 아니라 이들이 서로 작동하는 방식이나, 이체조건, 이체방법 등까지 세심하게 조종할 수 있다.

3. 속성/특성 (Attribute / Characteristics)

기존 비트코인과 동일한 속성



익명성(Anonymity) - 애초에 어떠한 개인정보도 입력하지 않기 때문에 개인정보유출의 염려가 없다.

무국경성(Borderlessness) - 네트워크 상에서 존재하는 것이므로, 국경에 구애받지 않는다. 따라서 범국가적으로 사용될 수 있다.

탈중앙성(Decentralization) - 중앙관리서버나 주체가 없다. 따라서 시스템을 장악하거나 변조하거나 유용할 수 없다. <네트워크 비교(오른쪽이 분산네트워크)>

분산네트워크(Distributed network) - 전체네트워크는 하나의 서버로 연결되는 것이 아니라 근처의 노드에 거미줄처럼 얽혀 있다. 단일한 공격점이 존재하지 않기 때문에, 중앙서버를 공격해서 시스템을 다운시키는 것이 불가능하다. (그림참조)
DDoS차단(DDoS attack-proof) - 수수료 시스템이 있기 때문에, DDoS공격을 통한 시스템 마비가 불가능하다. DDoS공격 등의 시스템 공격은 대부분 네트워크에서 처리할 수 있는 양보다 훨씬 많은 작업을 폭탄처럼 투하하는 것이다. 한번식 웹싸이트에 사람들이 몰리면, 웹싸이트가 마비된다고 하는 데, 이것과 동일한 원리라고 이해할 수 있다. 그러나 블록체인 상에서는 각 작업에 수수료를 청구하고 있으므로, 애초에 막대한 자본이 없다면 DDoS공격이 불가능하다.

분할성(Divisibility into pieces) - 화폐의 단위가 낮게 분할될 수 있습니다. 우리가 1천원짜리가 있는데, 700원의 물건을 샀다면, 1천원을 주고 300원을 거슬러 받는 수 밖에 없습니다. 그러나 비트코인 등의 암호화화폐(Crypto currency)는 처음부터 700원만 지불하는 것이 가능합니다. 뿐만 아니라, 원한다면 1원 0.1원 0.01원 등 무한히 단위를 낮출 수 있습니다. 디지털 상의 단위이기 때문에 가능한 부분이다.

투명성(Transparency) - 각 블록 안에 포함된 거래내역을 모두 조회할 수 있다. 또한 시스템이 구동되는 원리가 포함된 소프트웨어 소스자체가 모두 공개되어 있다. 따라서 모든 것을 투명하게 관찰하는 것이 가능하다.

기존 비트코인보다 진보된 속성

튜링완전성(Turing-Completeness) - 이더리움을 사용하는 과정에서 튜링완전한 언어를 사용할 수 있다. (더 자세한 내용은 하단에 서술)

플랫폼을 통한 응용성(DApps on Platform) - 하나의 서비스가 아니라, 서비스를 창조해낼 수 있는 거대한 플랫폼이기 때문에 무한한 응용이 가능하다. (더 자세한 내용은 하단에 서술)

스마트컨트랙트(자기강제적 언어(Self-Enforcing Language)) - 이더리움을 통해 여러가지 계약을 창조해낼 수 있으며, 해당 계약을 이행하는 것도 강제적으로 만들 수 있다. 즉, 파기할 수 없는 디지털 계약을 만들어낼 수 있는 것이다.

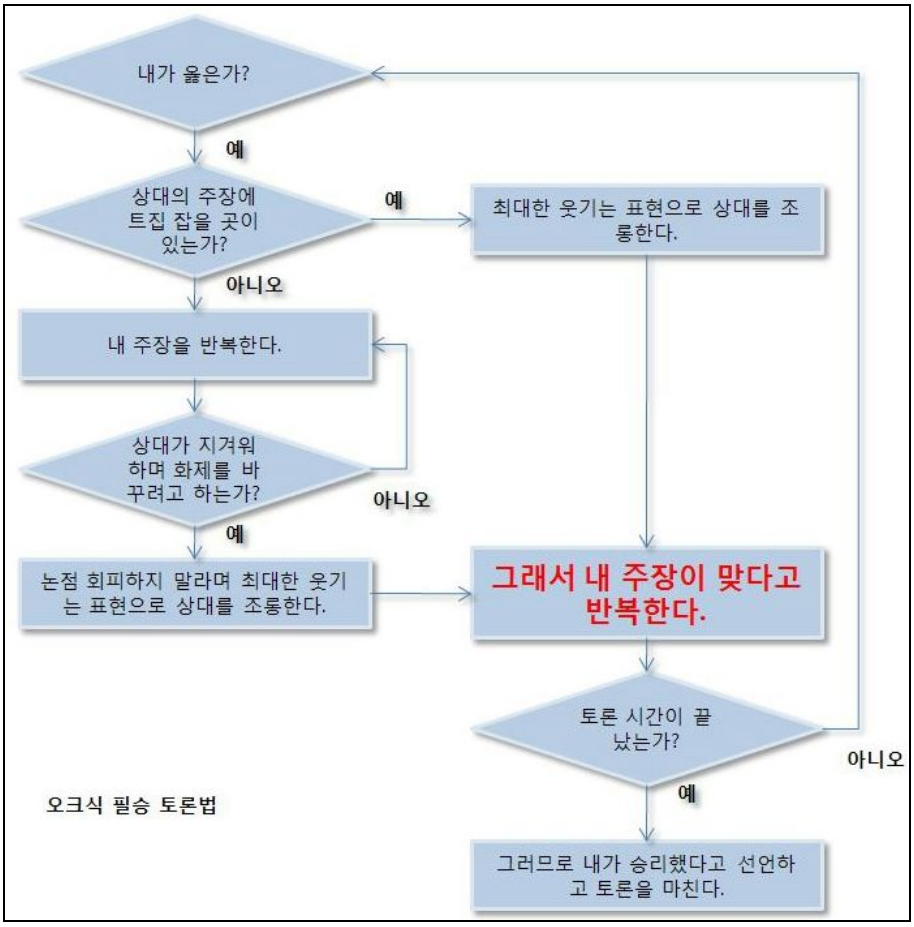
4. 튜링완전성(Turing-Completeness)
이더리움에서 대표적으로 자주 거론되는 특성이자 지금의 이더리움을 가능하게 만든 핵심개념이다. (대단해 보이지만 엄밀히 말하면 별로 특별하거나 새로운 개념은 아니다)

튜링완전성은 현재 범용컴퓨터의 시조격이라 할 수 있는 암호학자인 '엘런 튜링(Alan M. Turing)'으로부터 고안된 개념이다.

튜링머신(Turing Machine)
추상적인 수학 개념상의 기계이다. 튜링완전언어를 사용하며 무한한 저장공간이 있다면 이 세상의 모든 문제를 풀 수 있는 기계를 만드는 것이 가능한데, 그것을 튜링기계라고 부른다. 기본적으로 인간의 뇌도 동일한 방법으로 작동한다고 가정하였다.

튜링완전언어(모든 수학문제를 풀 수 있는 일반적인 알고리즘을 만들어낼 수 있는 컴퓨터언어) + 무한한 저장공간 = 모든 계산 가능한 문제를 계산해내는 기계 = 튜링기계(인간의 뇌)

튜링완전언어(Turing-Complete Language)
위의 튜링머신에 넣어야할 알고리즘을 만들 수 있는 언어가 튜링완전언어이다.



<알고리즘의 예-출처링크>

계산 가능한 모든 문제를 풀 수 있도록 하는 알고리즘을 만들기 위해서 충족되어야할 조건이 있다.

튜링완전언어는,
1) 프로세스를 충분히 분할할 수 있을 만큼 **작은 단위**를 사용할 수 있어야 한다.

2) **조건설정**과 **반복 명령어**가 있어야 한다.
if (조건문) + for/while 등 (루프문) = 무한루프(반복)가 가능 = 문제를 풀 때까지 영원히 멈추지 않는 알고리즘 설계가능
컴퓨터 프로그래밍 언어의 종류를 보면
'기계어(10110000 01100001)' - '어셈블리어(**mov al**, 061h)' - '절차적언어' 등으로 분류할 수 있다.

기계어나 어셈블리어의 경우, 충분히 작은 단위로 나뉘어져 있지만 실용성이 낮다.

반면 절차적언어는 실용성이 뛰어날 뿐만 아니라 어느정도 분할도도 충분히 높다. 따라서 일반적으로 대부분의 절차적언어-C언어, JAVA 등-는 '느슨하게 튜링완전(Loose Turing Completeness)'하다고 정의한다.

비트코인과의 비교
비트코인은 자체적으로 편집된 언어인 스크립트(Script)언어를 지원한다.

하지만 해당언어는 'if 명령문'만을 지원하며 자체적인 한계성도 지니고 있었기 때문에, 비트코인을 응용해서 활동하는 데에는 많은 제약이 따랐다.

그러나 이더리움은 자체적인 튜링완전언어들(Serpent, Solidity, LLL, Mutan)을 지원하고 있기 때문에, 사실상 상상가능한 모든 형태의 거래를 프로그래밍할 수 있다.

전혀 다른 차원 높은 자유도와 효율성을 누릴 수 있다.

4-1. 튜링완전의 이해(Understanding Turing-completeness)
왜 명령어의 분할도나 루프문(반복명령어)가 중요하다고 하는 것일까?

실생활에서의 예
실생활에서의 예를 통해, 이해할 수 있다.

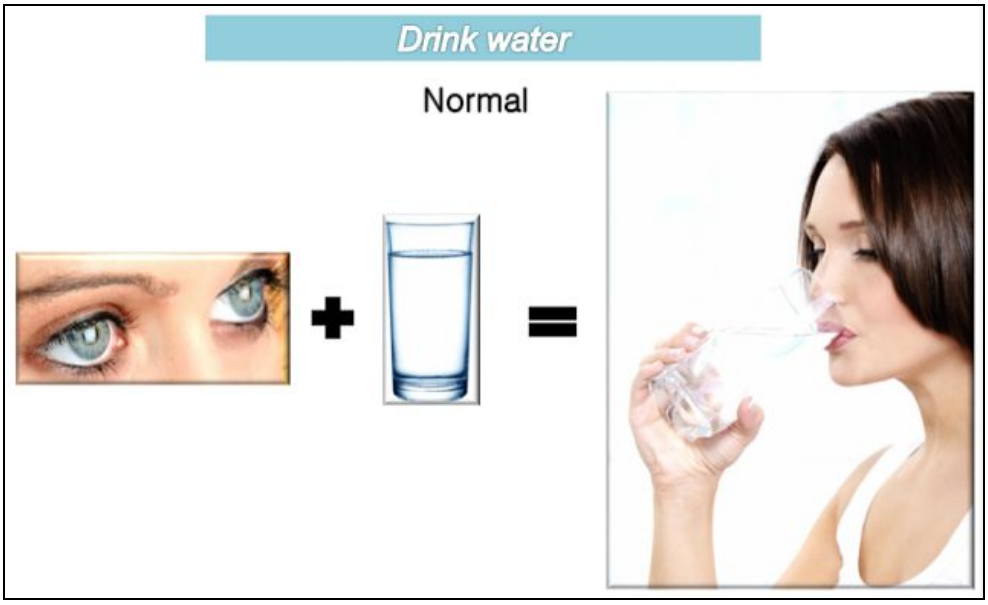
당신은 의자에 앉아서 테이블 위에 손을 편히 올려두고 있다. 그리고 목마름을 느끼며 앞에 있는 물이 가득 차 있는 컵을 바라본다. 그때 뇌에서 명령문 하나가 들려온다. "**저 컵의 물을 마셔라**"

"**저 컵의 물을 마셔라**"

이 명령문으로 당신이 그 컵의 물을 마시는 것 외에 달리 무엇을 할 수 있겠는가? 명령어가 너무 구체적이고 특정적이어서 다른 곳에 응용을 할 수가 없다.

우리는 그 컵의 물을 마실 때, '**그냥 마신다**.' 특별한 것 없다. 아래의 그림을 참조하자.

<그림1>



그런데, 실제로는 그렇게 간단했을까? 튜링의 시점에서 세상을 보면 어떨까?

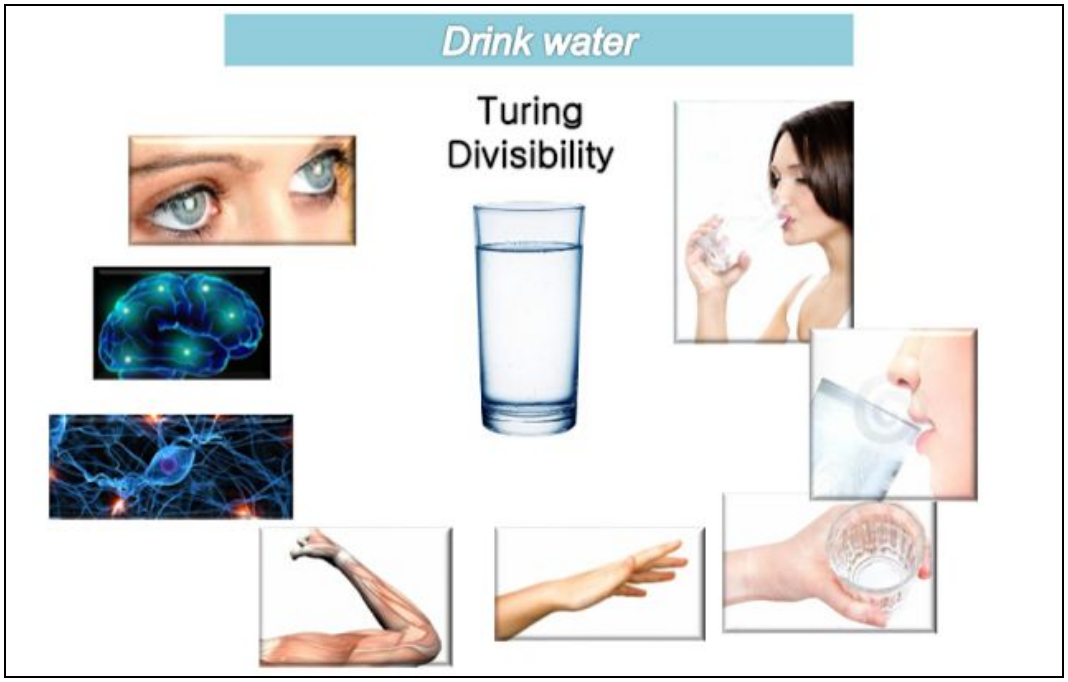
간단히 몇 단위로만 더 쪼개보자.

"**저 컵의 물을 마셔라**"라는 명령어는 사실 다음의 더 작은 여러가지 명령어로 이루어져 있다(또는 쪼갤 수 있다).

당신은 목마름을 느낀다 > 안구로 물을 존재를 확인한다 > 뇌에서 명령을 내리기 위한 전기스파크가 인다 > 해당 전기자극이 뇌의 뉴런과 시냅스를 거쳐 뻗어나간다 > 근육과 힘줄은 해당 명령을 수신한다 > 목표물체를 향해 손을 뻗는다 > 손을 뻗어 컵을 잡고 입 근처로 끌어온다 > 끌어온 컵을 향해 입을 벌린다 > 컵과 입의 각도를 조절하며 컵 안의 물을 입안으로 흘려 보낸다 > 인후(목구멍)는 들어오는 물을 꿀꺽꿀꺽 삼킨다

아래의 그림과 같을 것이다. (명령어의 분할)

<그림2>



이렇게 잘게 쪼개면 무엇이 좋을까?

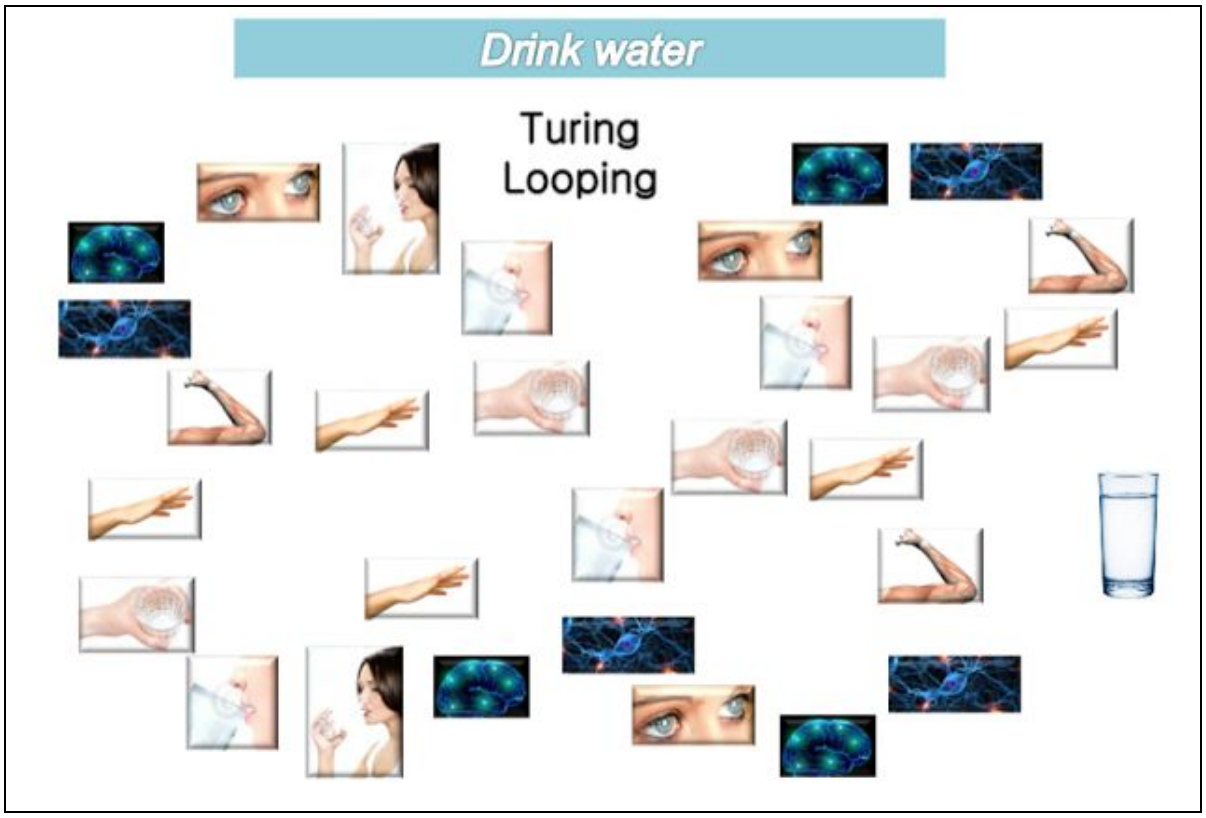
1) 각 과정의 중간 단계에서 '반복'이 가능해진다. 손을 뻗는 동작만 반복할 수도 있고, 물 컵을 잡다가 다시 신호를 보내 또 다시 잡을 수도 있다.

반복이 가능할 뿐더러, 한 과정을 시작해서 끝까지 마치는 것이 아니라 중간에 끊고 반복하는 것도 가능해진다.

2) 또한 응용성이 높아진다. "저 컵의 물을 마셔라"로써 할 수 있는 행위는 하나이지만, "손을 뻗는다"는 명령어는 물컵을 잡을 때 뿐 아니라, 농구를 할 때도, 도어벨을 누를 때에도, 연인의 머릿결을 쓸어줄 때에도 사용이 가능하다는 것을 알 수 있다.

반복의 경우를 다음 그림을 통해 살펴보자.

<그림3>



반복과 확장이 가능해졌다.

여기에 각 명령어를 여러곳에 적용하는 '**응용**'을 더해보자.

<그림4>

이 정도면 눈치빠른 독자는 알아챘을 것이다. 그렇다. 이것은 우리 인간이 작동하는 원리와도 일맥상통한다고 볼 수 있다.

즉, **튜링완전한 알고리즘**이다.

이것이 '엘런 튜링'이 기계에게 기대했던 것이고, 이 과정을 통해 인공지능 더 나아가서는 기계로 된 인간(로봇)을 만들 수 있다고 보았던 것이다.

다른 예
예전에는 청취를 위해 라디오를, 음악재생을 위해 오디오를, 녹음을 위해 녹음기를, 사진을 위해 사진기를, 게임을 위해 게임기를, 인터넷을 위해 컴퓨터를, 통화를 위해 전화기를 제각각 따로 사용하였다. - 튜링완전하지 않았기 때문이다.

그러나 튜링완전한 디바이스인 스마트폰이 등장하자 어떠한 변화가 생겼는가?

튜링완전하기 때문에 스마트폰 하나로 무한에 가까운 응용과 효율을 누릴 수 있게 되었다.

5. 무한루프 공격(DDoS)과 수수료 경제학 - Virtuous Circle
그러나 애초에 비트코인 응용언어에 무한루프문이 삭제된 이유는 무한루프를 통한 공격(DDoS 등)을 차단하기 위함이었다.

이더리움은 무엇이 달라서 튜링완전언어를 지원하면서도 무한루프 공격을 방지할 수 있는 것일까?

기존 비트코인의 경우, 비트코인을 '이체'하는 것에 대해서만 수수료를 물었다. 따라서 비트코인을 스크립트 언어를 이용해 다양한 기능을 추가해서 이체하여도 추가적인 수수료는 물지 않는다. 물론 제대로 된 응용기능 자체를 제공하지 않기도 했었지만 말이다.

이더리움은 모든 응용기능이 가능하다. 그러나 단순 이체 뿐 아니라 컴퓨팅자원을 소모하게 만드는 모든 응용기능을 실행하는데에 수수료를 물린다.

따라서 공격자가 시스템에 대규모의 작업을 투하하려면, 그 만큼의 수수료를 선불로 지불해야만 한다. 즉, 다음과 같은 논리가 성립하게 된다.

1) 공격자가 DDoS공격을 하기 위해 수수료를 투입한다.

2) 네트워크에 컴퓨팅파워를 투입하는 채굴자들의 수수료 수익이 증가한다.

3) 채굴자들의 수익이 증가하기 때문에 한계마진 시(=한계비용 제로)까지 더 많은 컴퓨팅 파워를 투입한다.

4) 높은 컴퓨팅파워로 인해 네트워크의 작업처리능력이 좋아진다.

5) 작업처리능력이 좋아졌기 때문에, 더 많은 공격을 처리할 수 있게 된다.

즉 이더리움의 수수료 시스템은, 외부에서 공격이 들어오면 오히려 네트워크보안을 더 강화하는 역할을 한다. - 선순환 시스템(Virtuous Circle)이 성립한다.

6. 스마트컨트랙트(Smart Contract)-자기강제적 언어(Self-Enforcing Language)

스마트 컨트랙트의 특징은 사용언어가 자기 강제적이라는 것이다.

우리는 다양한 상황에서 다양한 언어를 사용한다.

일반적으로 사용하는 구어,
공식적인 자리에서 사용하는 격식어,
서로 다른 나라간에 무역을 할 때 사용하는 인코텀즈(Incoterms),
법률 문서를 작성할 때 사용하는 법률언어 등이 있다.

일반적으로 계약 당사자들의 서명이 들어간 계약서는 법률언어를 통해 작성이 되는데, 혹시 누군가가 계약을 이행하지 않아도 직접적으로 강제로 이행하게 하는 방법은 없다.

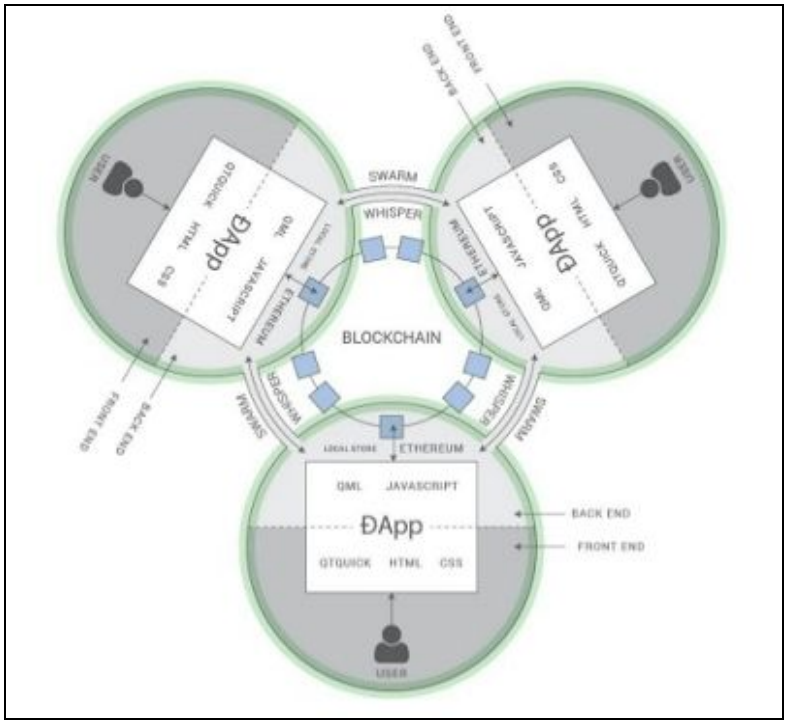
오직 간접적으로 소구권이나 저당권 등을 행사할 수 있을 뿐이다.

그러나 스마트컨트랙트는 이미 컴퓨터언어인 '실행 코드'들로 작성되기 때문에, 특정 조건이 달성되면 자동적으로 프로그램이 실행되어 계약이 이행된다. 즉, 시스템 상의 내용에 대해서는 계약이행이 강제된다.

이는 상대를 신뢰할 수 없는 경우의 계약에서 강력한 힘을 발휘할 수 있다.

7. 탈중앙화 앱 - DApp (Decentralized Application)

플랫폼화 된 블록체인 위에서 다양한 어플리케이션들을 구동시킬 수 있다.



그러한 어플리케이션은 '특성'인 익명성, 무국적성, 탈중앙화, 분산성 등을 모두 갖추게 된다.

이더리움 플랫폼 위에서 다양한 이종화폐를 제로에 가까운 수수료로 24시간 서비스하며, 즉시에 가까운 속도로 이체하는 것이 가능하다. 현재 외환 송금부터 입금확인까지 1주일이 걸리는 경우도 허다한데, 그러한 면에서 보면 가히 혁신이랄 수 있다.

여러가지 금융 상품들(채권, 주식, 파생상품 등)을 만들거나 거래하는 것도 가능할 것이다.

또한 여러가지 파일도 공유를 하고 판매를 할 수 있으며, 국가에서 직접적인 통제를 하는 것이 불가능하기 때문에 상당히 높은 자유도와 많은 가능성들이 있을 수 있다.

웹싸이트도 마찬가지이다. 이더리움 플랫폼 활용하는 웹싸이트를 만들 수도 있을 것이다. 그러한 익스플로러에서는 실시간 송금이 가능해지며, 서버 없이 컴퓨터 이용(cloud system)이 가능해질 수 있다.

7-1. 예시
몇 가지 실제 사례를 통해, 자세히 살펴보겠다.

1) SLOT Machine by JorisBontje - (시간절약을 위해 3:00부터)

슬롯 머신에 얼마를 투입했는지, 확률은 얼마인지, 결과가 어떻게 나왔는지 모두 투명하게 관찰할 수 있으며, 따라서 관리자가 취하는 부당한 이익을 막을 수 있게 된다.

2) Prediction Market by Atomrigs in Ethereumkorea - (시간절약을 위해 12:00부터)

한국인인 Atomrigs(예명)가 개발한 예측시장 작성 모듈이다.

이미 예시로 몇 가지 예측시장 상품이 작성되어 있다. 앞으로 일어날 일에 대해서 자유롭게 금융상품을 만들고 화폐를 충전할 수 있다.

3) **Adept by Samsung & IBM**

앞으로 사물인터넷(IoT)가 어떻게 이더리움 등의 블록체인 플랫폼을 통해 현실화가 될지 잘 알려주는 프로젝트 예시이다.

삼성과 IBM 두 공룡기업이 제작한 사물인터넷 구현에서는, Bittorrent(파일공유) / Ethereum(스마트 컨트랙트) / Telehash(메시지)가 프로토콜로 사용이 되었다.

8. 인터넷 위의 경제(Internet with Economy)
이제 직접적으로 인터넷 위에서 경제활동을 할 수 있게 된다. 이더리움을 통해 실시간으로 사물 간의 화폐의 이체가 가능해지며, 스마트 컨트랙트(Smart Contract)를 통해 각 사물 그리고 수 많은 주체들과 계약을 만들어서 자동화된 경제생활도 누릴 수 있을 것이다.

또한 이더리움은 인터넷상으로 진행하는 결제의 어려움을 완전히 없애버리며, 전세계의 모든사람과 실시간으로 경제활동을 할 수 있도록 돕는 강력한 엔진의 역할을 할 수 있을 것으로 기대된다.

중앙서버의 검열이나 통제 없이 각 주체 간 직접 연결 및 소통이 가능하다.

9. 더 많은 탈중앙화 앱 - DApps
앞으로 더 많은 것이 가능해질 수 있다.

현재로써는 요원한 일이지만 기술적으로만 접근하자면 다음과 같은 미래를 상상해볼 수 있다.

금융 DApps
상상가능 한 모든 자산을 블록체인 위에 올리고, 스마트 컨트랙트의 대상으로 사용한다.
-돈, 채권, 주식, 파생상품, 보험, 헷지컨트랙트, 유언장, 복권, 도박 등

준/비금융 DApps
직접적인 금융은 아니지만, 스마트 컨트랙트를 통해 활용될 수 있는 것들이다.
-토큰, 쿠폰, 자신의 이름으로 발행된 코인, 투표 등

탈중앙화 조직/회사(Decentralized Organization/Corporation)
회사나 조직을 블록체인 상에 올리고 운영한다.
-월급지급, 금전거래, 회계장부기록, 이사회녹음문서 기록, 지분표시, 투표 등을 투명하게 운영

탈중앙화 자율 조직/회사(Decentralized Autonomous Organization/Corporation)
고도의 인공지능(알고리즘)을 통해 자율적/자동으로 구동하는 조직/회사가 탄생할 수 있다.
-인공지능을 통해 운영주체 개입을 최소화하고, 블록체인 상의 알고리즘이 자체적으로 의사를 결정하여 영업, 회계, 구매, 판매 및 수익분배 등을 실현

이더리움 프로토콜은 온전한 P2P방식으로 온라인 세상에 참여할 수 있게 해주며, 중앙주체 없이도 또는 심지어 인간의 적극적 개입 없이도, 충분히 '인터넷'과 '그 위의 경제'가 실현되고 구동될 수 있음을 가능성의 수준에서 보여준다.

비트코인은 이미 성공적으로 중앙주체없는 화폐가 안정적으로 작동할 수 있다는 것을 기술적인 면에서 입증해왔으며, 현재도 그 세는 매일 증가하고 있다.

이를 통해 중앙주체의 존재로 인한 여러가지 폐단을 제거할 수 있었으며, 또한 중앙주체가 없을 때의 단점을 해결하는 다양한 방법을 제시해주고 있다.

기술적으로만 구현되었을 뿐이기 때문에, 실생활에서 온전히 적용이 되려면 단순히 사용자 경험이나 의식단계가 채워져야 할 뿐 아니라, 법을 포함한 제도적인 지원도 적극적으로 필요하다.

이더리움은 최신 기술 중 하나로, 앞으로 어떻게 사물인터넷이 구동하고 공유경제가 작동할 수 있을지에 대해 상상력과 통찰의 기반을 제공해준다.