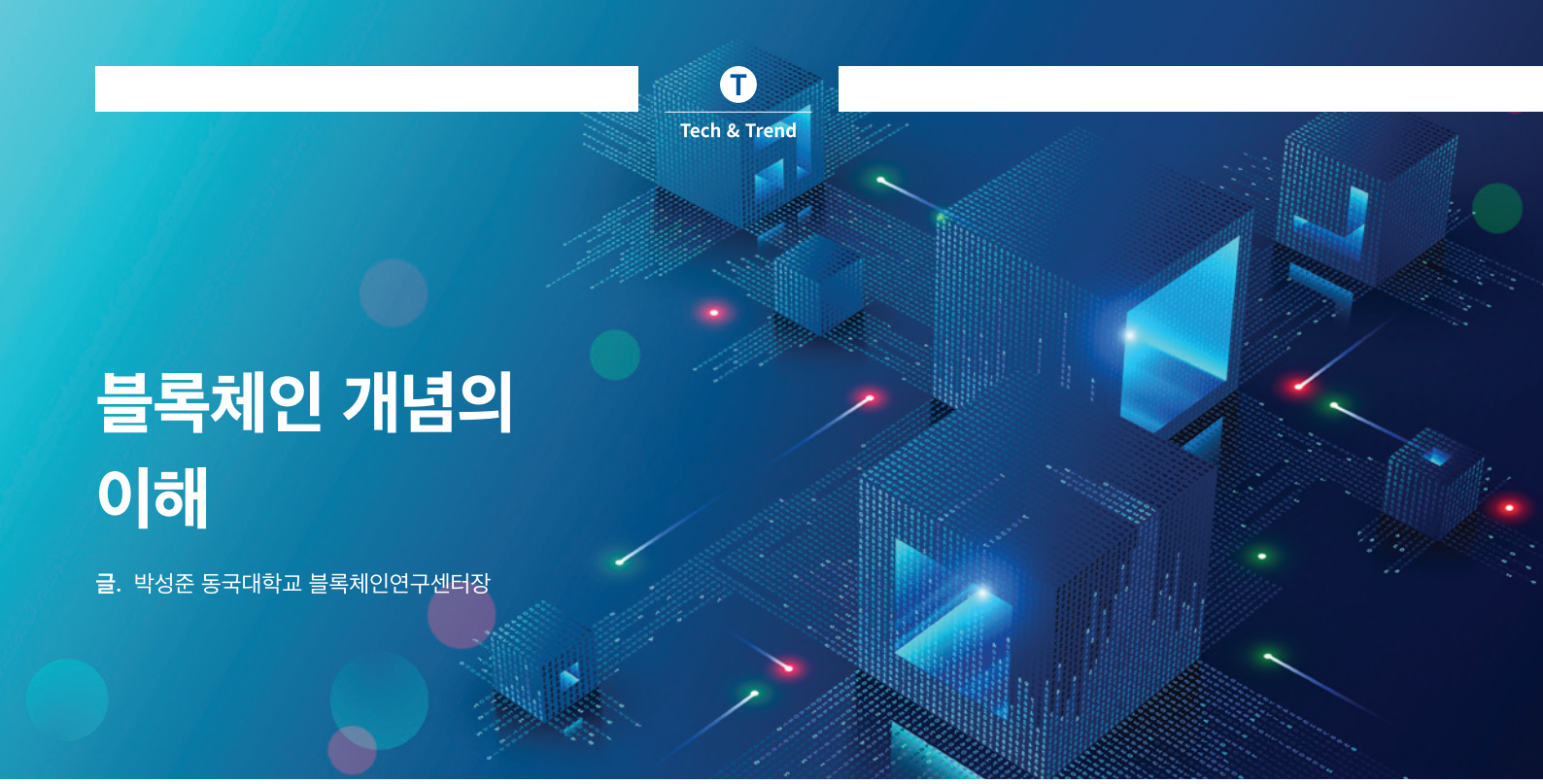

블록체인 개념의 이해

글. 박성준 동국대학교 블록체인연구센터장

개요

비트코인(Bitcoin)에서 창안된 분산원장(Distribution Ledger) 기술을 블록체인(Blockchain)으로 오해하는 경향이 매우 강하지만, 블록체인은 분산원장 이상의 개념을 포함하고 있다. 이런 연휴는 블록체인하면 암호화폐(Cryptocurrency), 암호화폐하면 비트코인으로 우리의 사고가 연결되기 때문이라고 생각된다. 그러나 암호화폐가 블록체인의 대표적인 응용서비스이긴 하지만, 블록체인은 단순한 암호화폐를 창출하는 기술을 넘어 우리에게 주어진 새로운 컴퓨터 개념으로 확장되었다. 블록체인을 새로운 컴퓨터로 이해할 수 있으면, 현재 전 세계적으로 진행되고 있는 블록체인 혁명은 어쩌면 당연하다고 생각하게 된다.

이 글에서는 블록체인 개념의 이해를 위해, 비트코인의 3가지 원리와 분산원장이 어떻게 새로운 컴퓨터인 블록체인으로 확장되는지에 대해 설명하고자 한다. 이러한 이해를 바탕으로 블록체인 혁명의 흐름을 블록체인 패러다임(Blockchain Paradigm)으로 명명하고, 블록체인 패러다임에 의해 우리의 세상이 어떻게 전환되고 있는지에 대해 개념적으로 설명하고자 한다.

블록체인이란?

비트코인

블록체인을 이해하기 위해서는 먼저 블록체인 개념의 시초인 P2P(Peer to Peer) 암호화폐 시스템 비트코인에 대한 이해가 필요하다.[1)]

비트코인은 화폐를 독점 발행하는 중앙기관(TTP : Trust Third Party)의 신뢰성에 대한 문제점을 해결하고자 화폐 발행 권한을 탈중앙화(decentralized)하고자 하는 생각에서 중앙기관 없이 신뢰성을 확보할 수 있는 P2P 암호화폐 시스템이다. P2P 암호화폐 시스템을 개발하기 위해서는 기본적으로 다음의 3가지 사항을 고려하여야 한다.

① 암호화폐 발행을 누가 어떤 조건으로 할 것인가?
② 암호화폐의 진위 판단은 어떻게 할 것인가?
③ 암호화폐의 이중지불(double spending) 문제를 어떻게 해결할 것인가?

이 3가지 고려사항을 최초로 해결한 것이 비트코인이다. 비트코인에서 3가지 고려사항을 해결한 방법은 다음과 같다.

① 암호화폐 발행을 누가 어떤 조건으로 할 것인가?

기존에 화폐발행 권한을 신뢰성을 가정한 중앙집중기관이 독점 발행하는 문제점을 해결하고자 화폐발행 권한을 누구든지 가질 수 있도록 화폐발행 권한을 탈중앙화한 것이다. 즉, 누구든지 화폐를 발행할 수 있다는 것이다. 그런데 누구든지 화폐를 마음대로 발행할 수 있다면 그것은 화폐로서의 가치가 없을 것이기 때문에, 누구든지 화폐를 발행할 수 있으나 발행조건을 추가함으로써 화폐로서의 가치를 인정받게 한 것이다.

그렇다면 언제 어떤 조건을 만족하였을 때 화폐를 발행할 수 있는지에 대한 합의가 필요하게 된다. 이러한 합의 조건이 비트코인의 혁신적인 아이디어이다. 비트코인에서는 화폐 발행 조건이 블록을 생성한 조건이 된다. 이는 이중지불 방지와 연계하여 설명할 것이다.

② 화폐의 진위 판단은 어떻게 할 것인가?

이는 우리가 가지고 있는 상식적인 생각에서 이해할 수 있다. 현재 우리가 사용하는 종이 화폐가 진짜인지는 어떻게 확인할까? 일반인들은 종이 화폐의 위·변조방지 기술을 믿고, 관행적으로 진짜라고 생각하고 있지만, 우리가 사용하는 종이 화폐가 진짜인 이유는 화폐발행 권한이 있는 한국은행에서 발행한 것이기 때문에 진짜인 것이다. 즉, 어떤 화폐가 진짜인 이유는 화폐발행 권한이 있는 기관에서 발행조건에 맞게 발행했다는 것을 의미한다.

비트코인의 위·변조 여부도 위의 생각과 동일하다. 즉, 암호화폐 비트코인의 진위를 판단하기 위하여 암호화폐는 발행 권한이 있는 자가 발행조건에 맞추어 발행된 것인지를 확인하면 된다.

그렇다면 암호화폐가 발행 권한이 있는 자가 발행조건에 맞추어 발행한 것인지를 어떻게 확인할 수 있을까? 이를 해결하기 위해 거래 체인(Transaction Chain) 개념이 도입된다. 암호화폐를 수신한 자는 암호화폐를 송신한 자에게 암호화폐의 출처를 문의한다. 암호화폐 송신자 또한 그 암호화폐를 누군가에서 받았을 것이고, 그러면 다시 그 누군가를 확인한다.

이러한 과정을 연속적으로 하게 되면 최종적으로 누구로부터도 암호화폐를 수신하지 않았음에도 불구하고 암호화폐를 가진 자가 있게 되며, 바로 이 최종적인 사람이 암호화폐를 발행한 사람이 되는 것이다. 거래 체인이란 바로 암호화폐의 진위를 확인하기 위해 출처증명을 요청하는 과정에서 생겨나는 암호화폐의 연속적인 유통을 의미한다.

이때 암호화폐를 발행한 사람이 우리가 합의한 발행조건에 맞추어 발행했으면 그 암호화폐는 진짜인 것이다.

③ 암호화폐의 이중지불 문제를 어떻게 해결할 것인가?

이제 마지막으로 암호화폐의 이중지불 문제이다. 이중지불 문제란 동일한 암호화폐를 반복해서 사용하는 문제이다. 당연히 암호화폐는 디지털정보이기 때문에 이중지불이 일어날 수 있다. 바로 이 이중지불 문제를 해결하기 위해 필요한 기술이 분산원장(또는 블록체인) 기술이다. 암호화폐를 수신한 사람은 암호화폐의 진위를 거래 체인으로 확인한다고 설명하였다. 문제는 자기가 수신한 진짜 암호화폐가 이중지불된 것이 아니라는 것을 확인해야 한다는 것이다.

'어떻게 하면 확인할 수 있을까?' 방법은 암호화폐 시스템에 참여한 모든 사람에게 물어보는 것이다. 모든 사람에게 물어본 결과 모든 사람이 자기보다 먼저 이 암호화폐를 수신하지 않았다는 답변을 듣게 되면 수신한 사람이 최초로 받은 암호화폐이며, 이는 바로 이중지불이 아니라는 것이 된다.

문제는 이러한 이중지불 확인을 위해서는 이중지불임을 알게 된 사람이 답변을 반드시 해야 하는데, '왜 답변을 해야 하는가'라는 문제가 다시 발생한다. 이러한 사유로 암호화폐는 답변을 하는 사람에게 답변을 하는 유인책으로 보상체계를 만들어 해결한다. 이것은 국가에서 시행하고 있는 포상제도와 유사한 개념이다. 결론적으로 암호화폐는 보상체계와 밀접한 관계가 있게 된다.

이때 많은 사람들이 이중지불을 발견한 사람이 거짓말을 할 경우에는 어떻게 하는가에 대한 질문을 한다. 이 문제는 암호화폐 거래가 일어나는 경우 이중지불을 방지하기 위해 모든 사람에게 물어봄으로써 이중지불 거래 여부를 모든 사람이 판단하는 방법으로 해결한다. 즉, 한 사람이 거짓말을 한다고 하여 이중지불이 발생할 수 없으며, 모든 사람에게 확인하여 이중지불이 아니라는 것을 다수결에 의해 결정함으로써 이중지불 문제를 해결할 수 있다는 것이다.
이때 이중지불 여부의 답변을 하기 위한 수단으로 블록(Block)이라는 개념을 도입한다. 블록이란 거래들의 집합개념으로 이중지불이 아닌 정당한 거래들의 모임이라고 생각하면 된다. 그리고 블록체인이란 생성된 블록들의 연결이 되는 것이다.

이더리움

비트코인에 대해 많은 사람들이 화폐인가 아닌가의 논쟁을 하고 있으나, 이것은 본질을 벗어난 논쟁이다. 비트코인의 본질은 우리에게 P2P 방식 모델의 실현 가능성을 보여줬다는 데에 있다. 지금까지 우리는 모든 생태계를 신뢰를 가정하는 중앙집중방식 모델로 구축하였다. 그러나 비트코인은 신뢰를 보장하는 중앙기관(제3의 신뢰 기관) 없이도 신뢰를 보장할 수 있는 P2P 모델도 가능하다는 것을 증명하였다. [그림 1]

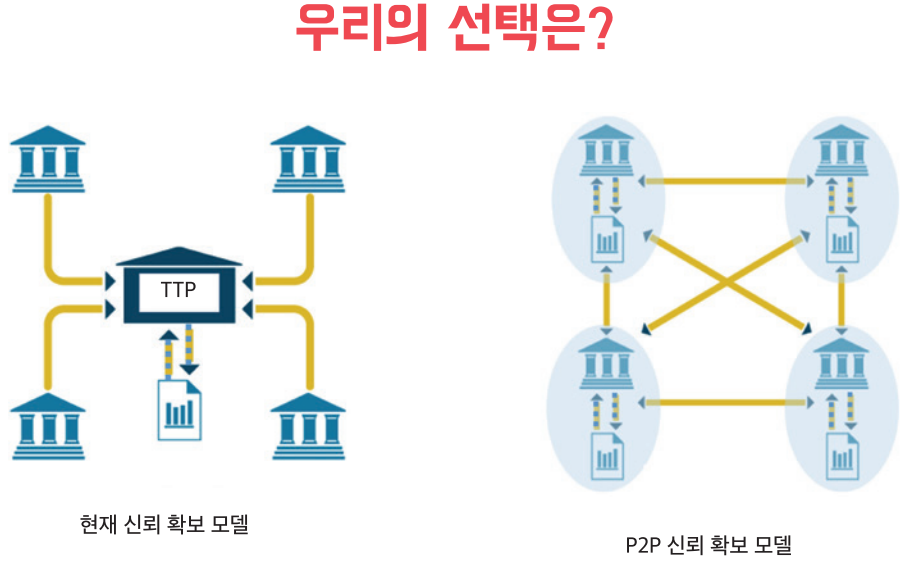

그림 1. 비트코인의 본질

이는 굉장히 중요한 의미를 내포한다. 현재의 모든 중앙집중방식의 다양한 문제점(과연 우리가 신뢰해야 하는 중앙기관의 신뢰성 문제 등)을 해결할 수 있는 단초를 제공하기 때문이다. 따라서 우리는 현재 중요한 결단을 해야 한다. 기존의 중앙집중방식 모델을 유지할 것인가? 아니면 P2P 방식으로 전환해야 할까?라는 판단의 기로에 있는 것이다.
비트코인이 탄생한 지가 10년이 지났다. 비트코인 탄생 이후로 전 세계적으로 중앙집중방식과 P2P 방식을 비교하였고, 결과는 P2P 방식이 더 우리의 가치(투명성, 공개성, 신뢰성 등)에 합당하다는 결론을 내린 것이다.(물론 아직 반대하는 사람들도 있음) 결론적으로 현재의 중앙집중방식을 P2P 방식으로 전환해야 한다는 것이다.
그러나 비트코인은 튜링 불완전성(Turing incompleteness) 등 많은 문제점을 가지고 있다. 한마디로 비트코인은 대다수 중앙집중방식을 P2P 방식으로 전환하는 데에 있어서 문제점을 가지고 있다는 것이다. 이러한 문제점을 해결하여 모든 중앙집중방식을 P2P 방식으로 전환할 수 있도록 비트코인의 튜링 불완전성 특성을 해결하여 튜링 완전성(Turing completeness) 특성을 갖도록 확장한 것이 이더리움(Ethereum)이다.[2)]

블록체인 정의

블록체인 정의를 이해하기 위해서는 먼저 튜링 완전성을 이해해야 한다. 튜링은 컴퓨터 모델을 창안하고 컴퓨터를 만든 사람이다. 일반적으로 튜링머신이란 현재 우리가 사용하고 있는 컴퓨터라고 간주하면 된다. 튜링이 컴퓨터를 만들었다는 사실보다 중요한 것은 튜링이 자신이 만든 컴퓨터의 한계를 증명하였다는 것이다. 컴퓨터의 한계를 증명하였다는 것은 컴퓨터가 할 수 있는 일과 할 수 없는 일을 구분하였다는 것이다. 튜링 완전성이란 컴퓨터가 할 수 있는 모든 것을 다하는 개념이고, 튜링 불완전성이란 컴퓨터가 할 수 있음에도 불구하고 못하게 제약을 했다는 것이라고 간단히 이해하면 된다.

비트코인이 튜링 불완전성을 갖는다는 의미는 컴퓨터가 할 수 있음에도 여러 가지 이유(해킹 방어 등)로 제약을 가지고 있다는 것을 의미한다. 이는 모든 중앙집중방식을 P2P 방식으로 전환할 수 없다는 것을 의미한다. 한편으로 비트코인의 튜링 불완전성 특성을 개선하여 튜링 완전성 특성을 갖도록 개선한 이더리움은 모든 중앙집중방식을 P2P 방식으로 전환할 수 있다는 것을 의미한다.

결론적으로 블록체인은 컴퓨터가 됐다고 생각하면 된다. 구체적으로 블록체인을 정의하면 다음과 같다.

블록체인이란 '글로벌 신뢰 컴퓨터(A Global Trust Computer)'

이해를 돕기 위해 블록체인이란 다수의 컴퓨터를 P2P 네트워크로 연결하여 하나의 컴퓨터처럼 동작하는 가상의 월드컴퓨터라고 이해하면 된다. 따라서 블록체인은 우리에게 주어진 새로운 컴퓨터이자 네트워크이다. [그림 2]

그림 2. 블록체인 : 컴퓨터이자 네트워크

블록체인 패러다임과 사례

블록체인 패러다임

2장에서 설명하였듯이 블록체인은 글로벌 신뢰 컴퓨터로 간주할 수 있다. 이는 블록체인으로 무엇을 할 수 있는가의 근본적인 질문에 대해 간단한 답변을 제공한다. 블록체인을 우리에게 주어진 새로운 컴퓨터이자 네트워크라고 생각하면, 블록체인이 창출하는 서비스의 한계는 현재 컴퓨터가 창출하는 서비스의 한계와 동일하게 되며, 모든 것이 블록체인의 응용서비스가 된다는 것을 의미한다. 간단히 현재 스마트폰 생태계와 블록체인 생태계를 비교하면 다음 그림과 같다. [그림 3]

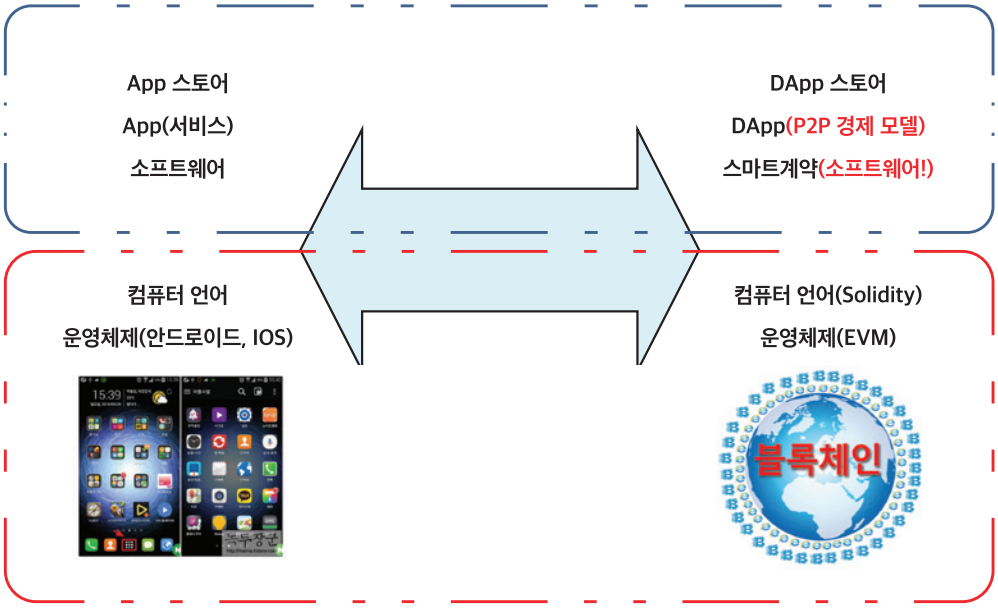

그림 3. 스마트폰 생태계와 블록체인 생태계 비교

이러한 관점에서 현재 컴퓨터와 인터넷 기반으로 창출되는 모든 서비스를 블록체인 기반으로 재창출할 수 있게 되며, 이러한 흐름을 블록체인 패러다임(Blockchain Paradigm)이라고 명명한다.

사례

이제는 모든 사람이 알고 있듯이 블록체인 패러다임의 대표 사례로는 암호화폐가 있다. 비록 암호화폐의 부정적인 측면이 있으나, 암호화폐의 중요성 및 필요성에 대해서는 다음에 설명하기로 한다.

국외의 경우 이더리움 기반의 응용서비스가 가장 활발히 창출되고 있는 실정이다. 현재까지 이더리움 기반 응용서비스는 약 2,500여 개가 창출되고 있으며, 실제 이더리움 사용자는 약 83,000명/일 이상, 거래량은 약 200만/일 정도이다.

물론 2,500개의 창출서비스 분야에는 금융, 물류, 에너지, 게임 등 대부분의 분야가 포함되어 있다. 창출 분야를 서비스 분야로 분류하면, 게임 분야가 509개 도박 분야가 379개 금융 분야가 265개 등이다. [그림 4]

국내의 경우 정부의 블록체인 육성 정책에 의해 한국전력의 P2P 전력거래망 및 전기자동차 충전인프라 사업, 교보생명의 실손 보험에서의 P2P 실시간 보상서비스 등 많은 서비스가 구축되고 있다. 은행연합회 또한 기존의 공인인증서를 대체하는 블록체인 기반 인증서 뱅크사인을 구축하여 서비스 중이며, 다른 한편으로는 대표적인 블록체인 기반 서비스가 될 것으로 간주하는 암호화폐를 활용한 해외송금 서비스의 경우 정부 정책에 의해 서비스 시행이 금지되어 있다.

결론

블록체인을 글로벌 신뢰 컴퓨터로 정의하였다. 그리고 블록체인을 컴퓨터로 이해하는 순간 현재 우리가 컴퓨터를 활용하여 서비스를 창출하는 방법과 유사하게 블록체인 기반 서비스를 창출할 수 있다. 현재 전 세계적으로 다양한 분야에서 블록체인을 활용한 응용서비스가 창출되고 있으며, 이러한 흐름을 블록체인 패러다임이라 명명하였다.

블록체인 패러다임의 관점에서 우리나라도 조속히 블록체인 진흥정책을 추진하여야 한다. 그리고 블록체인 진흥정책에는 반드시 암호화폐 활성화 정책도 포함되어야 한다. 현재 정부는 암호화폐와 블록체인 진흥정책에서, 암호화폐의 ICO(Initial Coin Offering) 금지 등 강력한 규제 및 블록체인 활성화라는 이원화 정책을 추진하고 있다. 그러나 이는

암호화폐 및 블록체인의 잘못된 오해에서 출발한 본질적으로 잘못된 정책이다. 어떠한 타당한 근거도 없는 정부의 암호화폐의 부정적인 강력한 규제 정책은 블록체인 패러다임 흐름에 역행하는 것이며, 국내 블록체인 생태계를 죽이는 것이다.

Categories

Category	Total DApps	Monthly active users	Transactions (30d)	# of contracts
Exchanges	190	48.91k	497.16k	486
Finance	265	32.29k	134.96k	2.08k
Games	509	25.52k	675.97k	1.31k
Wallet	94	18.05k	52.97k	31
Gambling	379	11.77k	404.13k	1.26k
Development	167	9.42k	31.44k	49
Media	138	7.09k	28.64k	138
Storage	55	6.93k	27.56k	23
Social	273	4.42k	20.2k	181
Governance	65	4.23k	11.83k	32
Property	74	3.53k	49.37k	71
High risk	224	2.63k	14.45k	236
Security	72	2.12k	8.85k	21
Identity	32	1.24k	3.63k	20
Marketplaces	18	1.18k	8.24k	21
Energy	26	382	793	5
Insurance	21	119	529	4
Health	20	0	0	6

그림 4. 이더리움 기반 창출서비스 분야별 통계

혹자는 암호화폐를 제외하고는 블록체인의 가치가 없다는 극단적인 주장을 하는 사람들도 있으나, 이는 매우 근시안적인 잘못된 생각이다. 블록체인을 활용한 응용서비스 창출은 우리의 상상력과 창조력에 의해 어떤 서비스가 창출될지는 모르나 매우 무한하다는 것만은 확실하다.

우리나라의 블록체인 경쟁력을 확보하기 위해서는 조속히 정부의 본질적으로 잘못된 암호화폐 규제 및 블록체인 활성화라는 이원화 정책을 암호화폐와 블록체인 활성화, 암호화폐 역기능 방지라는 원칙에 충실한 정책으로 전환해야 한다.

참고문헌

1) S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. https:// bitcoin.org/bitcoin.pdf, Dec 2008.

2) 이더리움 : www.ethereum.org