SPRi 이슈리포트

2015. 8. 24. (2015-006호)

비트코인2.0 - 기술 및 산업 전망

김정민 연구원
(jungmink26@spri.kr)

SPRi 소프트웨어정책연구소
SOFTWARE POLICY & RESEARCH INSTITUTE

○ 본 보고서는 「미래창조과학부 정보통신진흥기금」을 지원받아 제작한 것으로 미래창조과학부의 공식의견과 다를 수 있습니다.

○ 본 보고서의 내용은 연구진의 개인 견해이며, 본 보고서와 관련한 의문사항 또는 수정·보완할 필요가 있는 경우에는 아래 연락처로 연락해 주시기 바랍니다.

- 소프트웨어정책연구소 연구2실 김정민 연구원(jungmink26@spri.kr)

《 요 약 문 》

○ 암호 화폐 비트코인(Bitcoin)은 다양한 사회적인 이슈 및 회의적인 시각에도 불구하고, 해외에서 안정적인 대안화폐로서의 정착을 이루고 있는 상태임

○ 한편, 해외에서는 비트코인의 원천기술인 블록체인(Blockchain)이 비트코인 시스템에 국한된 기술이 아님을 강조하며, 중앙 관리형 시스템 전반을 분산화 할 수 있는 P2P 네트워크 기반의 비트코인 2.0에 주목하고 있음

○ 블록체인의 핵심기술은 “사용자간 분산 합의 시스템”, “채굴”, “거래장부 동기화 시스템” 총 3가지 요소로 나누어 생각할 수 있음

○ 이더리움(Ethereum)은 블록체인 응용 서비스의 수요를 충족시켜주기 위한 API 및 완전튜링언어를 제공하는 플랫폼으로서 2015년도 4월부터 현재까지 순차적인 서비스 오픈이 이루어지고 있음

○ IBM과 삼성을 필두로 IoT의 실현을 위한 블록체인 플랫폼인 ADEPT를 계획 중에 있으나, 현재 국내에서의 관련 기술 및 개념에 대한 관심이 부족한 실정임

○ 중앙 관리형 시스템과 반대되는 특성을 지니며, 핀테크(FinTech)와 밀접한 연관이 있는 본 기술에 대한 이해와 전망을 통하여 제2의 핀테크 규제 이슈가 발생하지 않는 것이 중요함

《 목 차 》

《 그림목차 》

1. 화폐로서의 비트코인

가. 비트코인(BitCoin) 개요

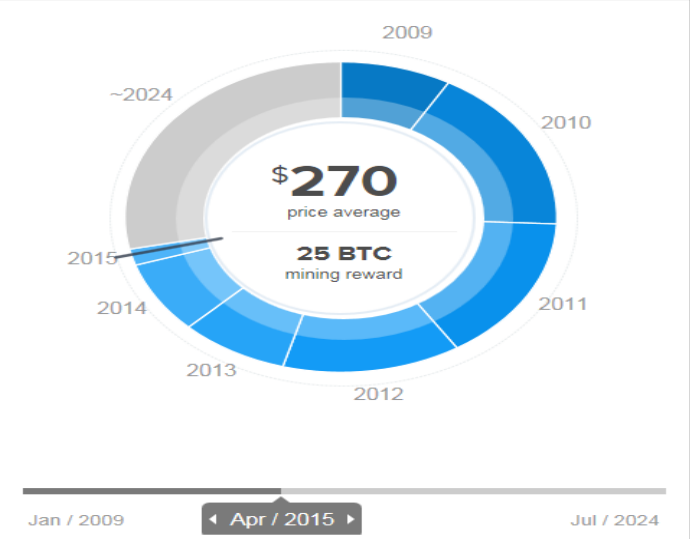
□ 비트코인은 나가모토 사토시(Nakamoto Satoshi)[1]에 의해 고안 된 총 발행량의 한계가 있는 암호화 된 디지털 화폐이며, 통화 단위는 BTC임

□ 비트코인의 특징

○ **(관리주체가 없는 시스템)** 중앙은행의 역할을 하는 별도의 시스템 및 서버가 존재하지 않기 때문에 사용자들의 합의를 통해 통화의 발행, 거래, 검증이 이루어짐

○ **(총 통화량 제한)** 비트코인은 화폐 발행량의 한계가 2,100만 BTC로 정해진 시스템으로서 기존 통화의 인플레이션/디플레이션 문제를 자동화된 시스템에 의한 발행(채굴)으로서 해결함

그림 1 비트코인 화폐 발행량(2015년 4월 기준)



출처 : http://www.coinbase.com

○ **(공개된 거래내역)** 익명성을 보장하지 않는 시스템으로서 모든 비트코인 사용자는 세계에서 일어난 거래 내역 일체를 가짐

1) 나가모토 사토시(Nakamoto Satoshi) : 비트코인 이론을 처음으로 제안했다고 비트코인사에서 주장하는 실존여부가 불확실한 인물. 실존인물인지 여부에 대한 많은 관심이 집중 되었으나 밝혀진 바가 미미함. 이름으로 추정하건데, 비트코인 서비스를 처음 구현한 개발자의 일본 지인의 이름을 따온 것이라는 설이 가장 유력하나 정확히 밝혀진 바 없음(https://en.bitcoin.it/wiki/Satoshi_Nakamoto 참고 후 의역)

- 비트코인을 통한 거래가 성립될 시, 모든 사용자는 이 거래내역을 자신의 장부(비트코인 지갑)에 자동으로 저장하게 되어 있음
- 실제 거래자의 신상정보와 장부에 기록 된 거래와의 매칭을 지원하지 않으나 언제 어떤 거래가 이루어 졌는지는 모두 공개되기 때문에 완전한 익명성 보장이 된다고 볼 수 없음

○ **(개인정보 불필요)** 비트코인 계정 생성에는 이름, 연락처, 주소 등의 개인정보를 요구하지 않음

- 계정 생성은 자신을 증명할 수 있는 수단을 부여하는 절차이며, 자신의 신상을 시스템에 입증할 필요성이 없음
- 그러므로 계정에 기입한 정보로 인한 제 3자의 개인정보 유출 문제가 발생할 수 없는 구조임
- 개인정보 거래를 통한 수익모델이 존재하지 않기 때문에, 비트코인 사용을 위한 이용자의 비용은 미미하며, 기존 자산 및 타 유사코인과의 환전 수수료가 수익원인 환전소 중심으로 관련 산업이 발전됨

○ **(강력한 보안성)** 중앙은행이 없는 분산화 된 합의 시스템은 거래 내역 조작, 단일 사용자 계정에 대한 해킹에 매우 강력한 보안을 제공함[2)]

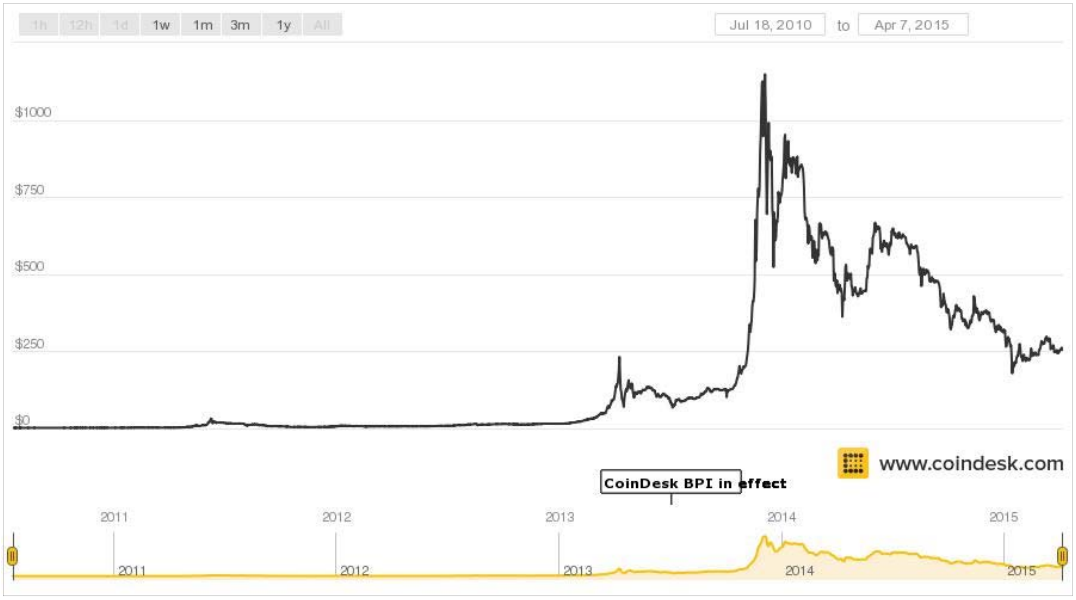
- 각각의 거래는 '검증 가능 상태'인 모든 사용자로 하여금 거래의 타당성 검증을 받으며, 이 과정에서 과반수의 거래 타당성 승인이 이루어 졌을 시에만 해당 거래가 성립됨
- 부정한 거래 조작 또는 해킹을 위해서는 '검증 가능 상태'인 사용자 소유 컴퓨팅 파워의 51% 이상을 장악해야 과반수 승인을 얻을 수 있음
- 비트코인 사용자의 수가 많아질수록 검증을 수행하는 기기가 세계 전역으로 분산되므로 독단적인 범법행위에 대한 시스템 내의 잘못된 승인이 발생할 확률이 극단적으로 감소

2) Protect your privacy, https://bitcoin.org/en/protect-your-privacy

나. 현황

□ 비트코인의 통화 가치는 2014년 민간 피해사례의 언론보도와 함께 신뢰성의 하락과 맞물려 폭락했다가 2015년을 기점으로 서서히 반등하는 추세임

그림 2 비트코인 환율 변화 추이(2011 ~ 2015)



출처 : www.coindesk.com

○ 2013년 12월 1BTC기준 1163달러였던 것에 비하여, 2014년 ~ 2015년 사이에 약 1/5수준인 250달러로 급락

○ **(사회적 부작용)** 규제망을 벗어나기 위한 용도로 사용

- 자신 소유의 계정이 아닌 새로운 거래 계정을 소유할 시, 거래내역 일체가 공개되어도 그 거래가 누구에 의해 이루어진 건지 알 수 없음
- 중앙은행의 자금 추적으로부터 자유로운 점에 착안한 마약거래 및 사회적으로 부적절한 실물거래의 수단으로 사용됨[3)]
- 또한, 개인정보를 요구하지 않는 비트코인의 특성을 이용한 부정한 자금의 세탁용도로 활용[4)]

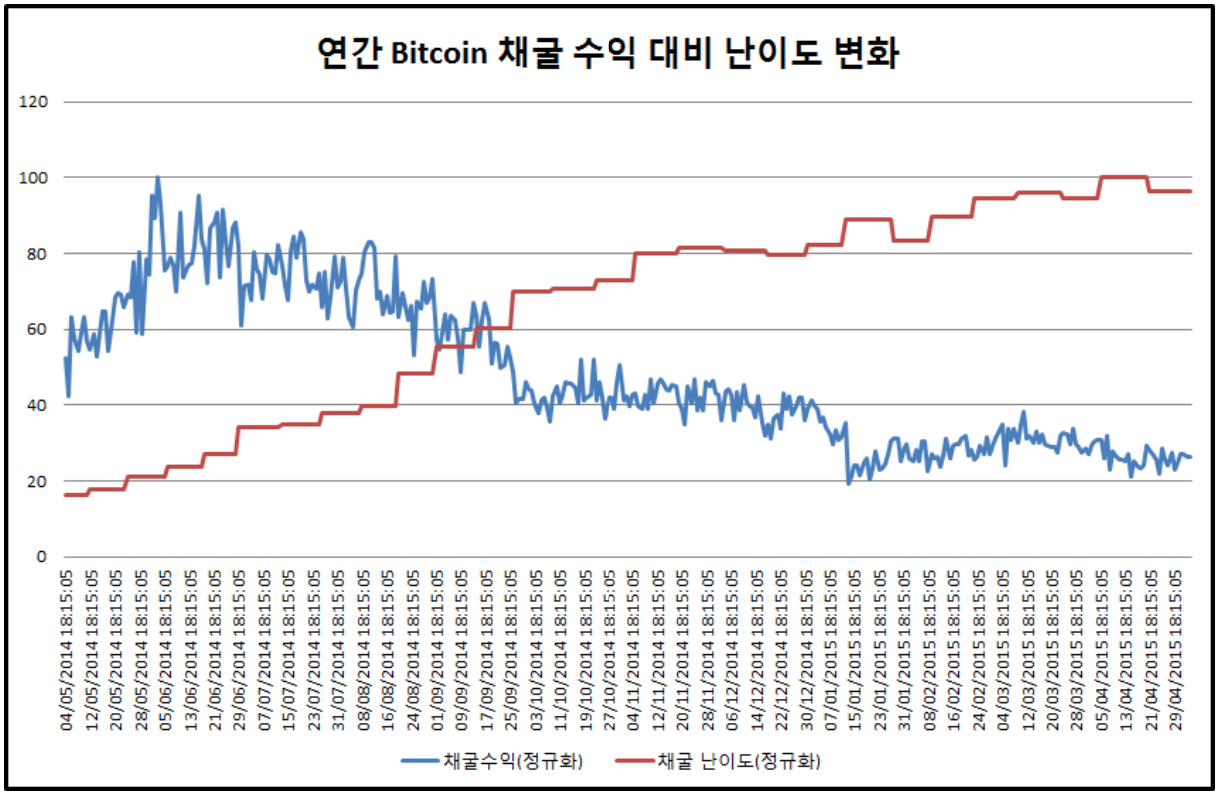
3) http://news.kbs.co.kr/news/NewsView.do?SEARCH_NEWS_CODE=3039231
4) http://www.wired.com/2014/04/dark-wallet/

○ **(시스템 신뢰성 저하)** 2014년 2월 해킹에 의하여 세계 최대 비트코인 거래소 마운트곡스가 약 4억 7천만 달러의 BTC를 도난당했다 주장함

- 당시 사건으로 인해 약 300달러 수준의 환율 급락이 이어지고, 비트코인의 신뢰성이 하락
- 그러나 2015년 1월 1일, 일본 경찰 측의 조사 결과를 토대로 마운트곡스 거래 시스템에서 사라진 비트코인은 해킹이 아닌 내부 시스템 부정 조작 때문으로 밝혀짐

□ 채굴을 위해 필요한 컴퓨팅 파워 및 소비전력은 비트코인의 발행률이 발행 한계량에 가까워짐에 따라 기하급수적인 증가세를 보임

그림 3 '14~'15년도 Bitcoin 채굴 수익 대비 난이도 변화



자료 : blockchain.info에서 인용 후 재정리

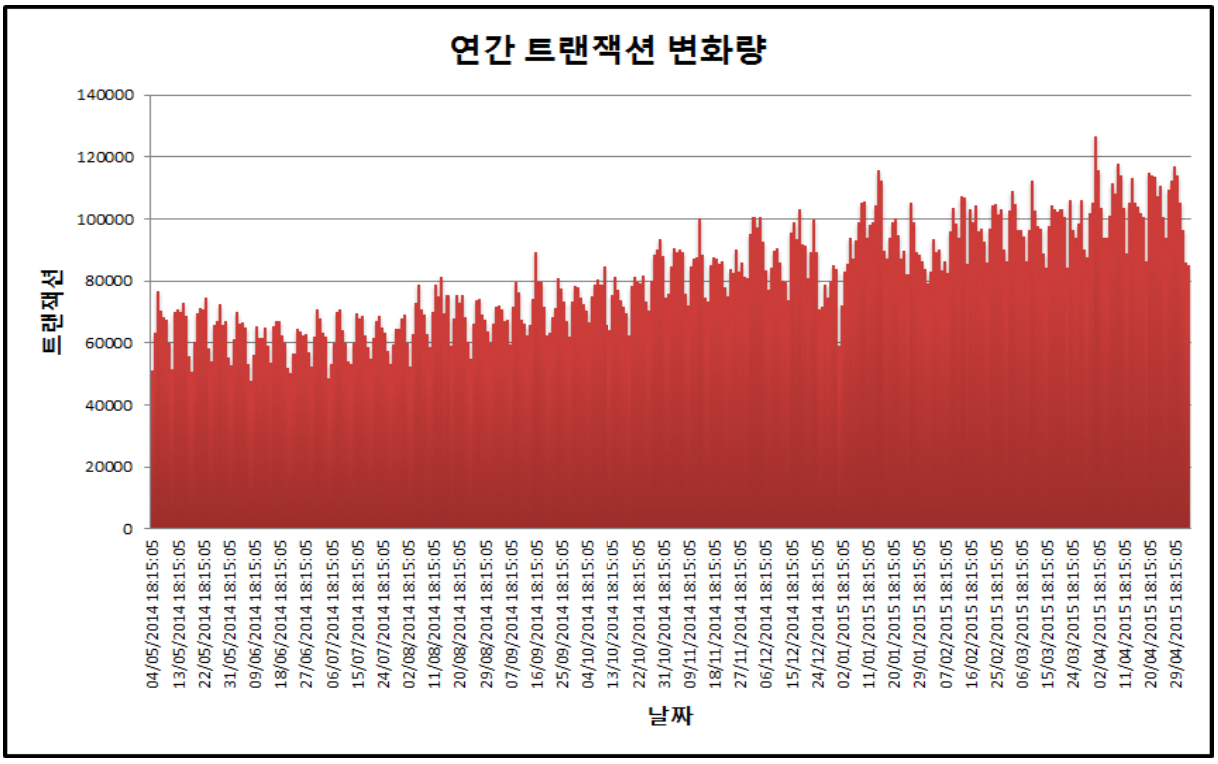
○ 비트코인 초창기 사용자는 개인용 컴퓨터 성능 수준으로 채굴이 가능했으며, 채굴의 보상으로 각 개인이 코인을 받을 수 있었음

○ 비트코인 거래가 시작 된 2009년 이후 매월 전월 기준 69%의 채굴 난이도 향상이 꾸준히 이루어 졌으며, 2015년을 기준으로 채굴 전문 업체를 제외한 채굴시도는 거의 사라진 상태임

○ 결과적으로 비트코인의 채굴 시장은 이미 레드오션이라 평가하는 의견이 지배적임

□ 위와 같은 상황에도 불구하고 비트코인을 통한 거래량은 꾸준히 상승 중

그림 4 '14~'15년도 Bitcoin 거래량 변화



자료 : blockchain.info에서 인용 후 재정리

○ 통화 가치는 비트코인 이용자의 신뢰도와 비례하여 불안정한 추세를 이어갔으나, 전체 거래량은 통화가치와 독립적으로 꾸준한 증가세를 보임

○ 채굴 난이도 향상으로 인한 보상 개념의 약화 및 사회적인 피해사례로 인한 신뢰도 하락에도 불구하고 사용량이 오히려 늘고 있는 현상은, 비트코인이 신용자산으로서의 가치가 점진적으로 인정 될 가능성이 있음을 시사

다. 비트코인의 한계

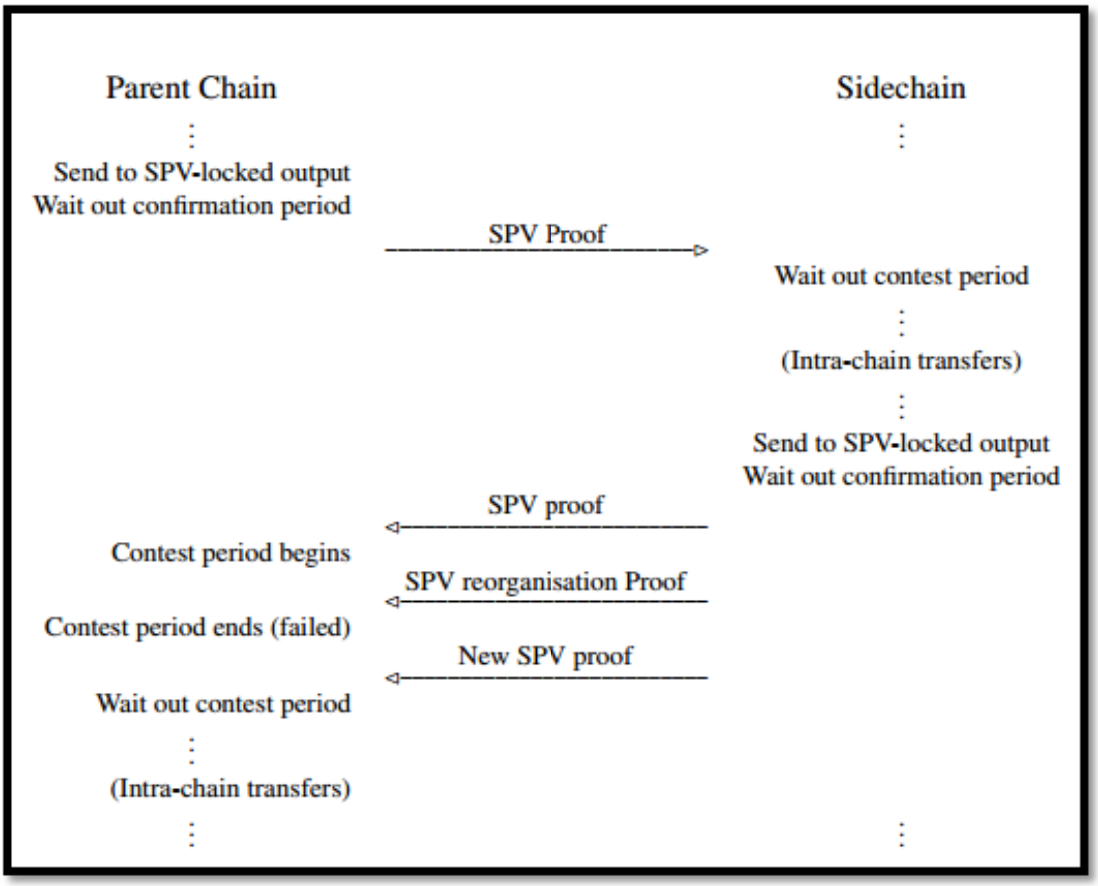
□ 폐쇄적인 시스템으로서의 변모

○ 화폐의 특성상 다양한 서비스를 위한 부가기능 제공에 소극적임

- 화폐로서의 가치 인정을 위해서는 현행 중앙은행에 의해 통제되는 화폐만큼의 신뢰성 확보가 중요
- 시스템의 원천 기술에 기반을 둔 다양한 응용 모델의 출현이 가능하나, 현재 가상화폐 시장 점유율의 88%[5]이상을 확보한 비트코인은 이러한 응용 모델의 시도로 인한 시스템 불안전성을 회피하는 전략을 취함

□ 사이드체인(Side-Chain)을 통한 한계 극복 시도

그림 5 Two-way pegged Sidechain 프로토콜



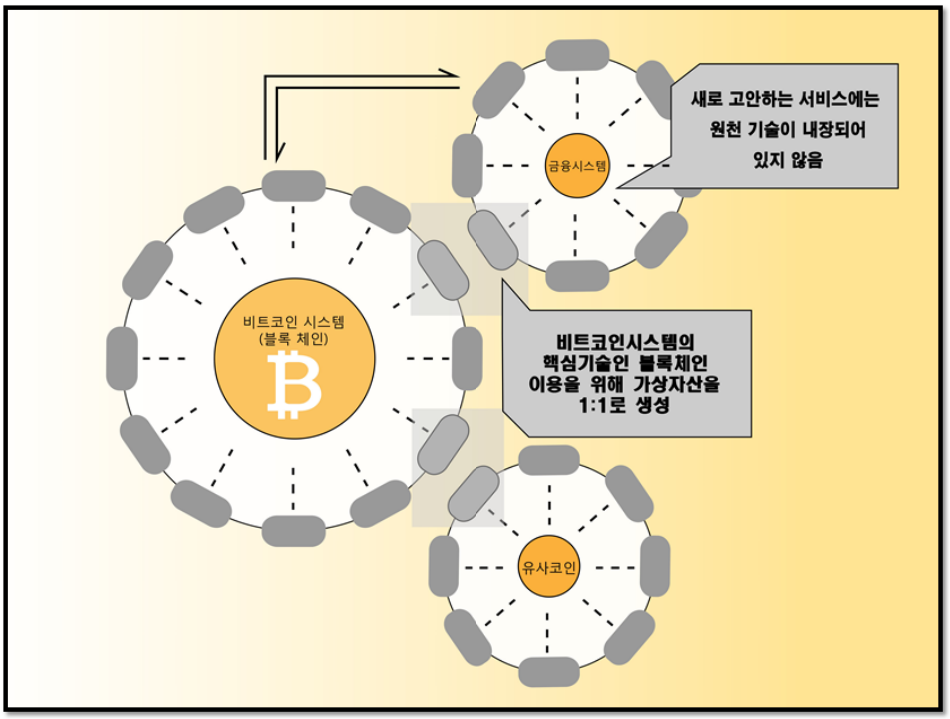
출처 : "Enabling Blockchain Innovations with Pegged Sidechains," 2014

5) http://coinmarketcap.com/currencies/views/all/

○ 동종업계 후발주자를 통해 기존 암호 화폐 시스템을 넘어서는 부가기능 제공 방법 등장

* 주식, 채권 등의 화폐 이외의 자산 개념을 도입

그림 6 사이드체인(Sidechain)의 원리



자료 : 소프트웨어정책연구소

- 원천 기술의 신뢰성을 다년간 검증한 비트코인의 시스템을 그대로 차용, 시스템 외곽에 채굴기능이 없는 새로운 거래 서비스를 만들어 비트코인 계정과 1:1 연결[6)]
- 채굴을 포함한 신뢰성 검증 기술은 비트코인에게 맡겨서 처리하고, 처리 된 거래 결과를 외곽에서 1:1로 받아옴으로써 새로운 서비스를 제공
- 비트코인의 원천 기술의 명칭이 “블록체인”이며 이 기술을 외곽에서 빌려 사용하기 때문에, 이러한 서비스를 “사이드 체인”이라 명명하고 있으며, 신뢰성을 차용함과 동시에 실험적인 서비스 구현이 가능하다는 장점이 있음

6) A. Back, M. Corallo, Enabling Blockchain Innovations with Pegged Sidechains, www.blockstream.com

라. 요약 및 시사점

□ 비트코인은 거래량 및 환율 추이를 토대로, 당분간 현 상태를 유지하며 점진적인 성장을 이룰 것

□ 비트코인은 공개 SW의 일종이나, 신뢰성이 이슈가 됨에 따라 안정성이 강화되는 반면 직접적인 응용사례 개척에는 폐쇄적인 시스템으로 진화함

□ 일반 대중이 전통적인 화폐 개념에서 탈피하는데 까지는 신뢰성 확보기간이 오랫동안 필요할 것으로 보이나, 원천 기술의 아이디어에 기반을 둔 새로운 서비스 유형이 나타나 서비스 되고 있음

□ 한편, 비트코인이 사회적인 이슈가 아니었던 국내에서는 디지털 화폐의 개념조차 대중에게 일반적이지 않음

□ 핀테크(FinTech)가 급진적으로 국내에 적용되고 있는 상황을 고려할 때, 비트코인의 응용 서비스가 적응 기간 없이 국내에 유입될 가능성이 존재함

○ 기술의 장점을 수용하기 이전에 표면적으로 드러날 가능성이 있는 다양한 부작용을 규제하여 도입자체를 막게 될 우려가 있음

□ 그러므로 일반 대중에게 화폐로서만 인식된 비트코인의 원천기술이 무엇인지와, 이를 토대로 어떠한 서비스가 가능한지 파악할 필요성이 있음

2. 비트코인의 핵심 기술

□ 비트 코인의 근본적인 혁신은 중앙의 권위와 제 3자의 보증(Centralized Trusted 3rd Party)에 의존하지 않음에도 가치를 전송하는데 있어 시스템적 신뢰성을 높이는데 성공한 것임

□ 이러한 탈중앙화 된(Decentralized) 시스템을 가능케 한 기술이 블록체인(Block-Chain)으로 정의한 알고리즘임

가. 블록체인의 정의

□ 블록(Block)으로 거래내역이 간주되며, 각 계정의 거래내역은 모두 시계열 순으로 체인(Chain)처럼 연결되어 관리된다는 의미에서 이 기술을 블록체인(BlockChain)이라 칭함

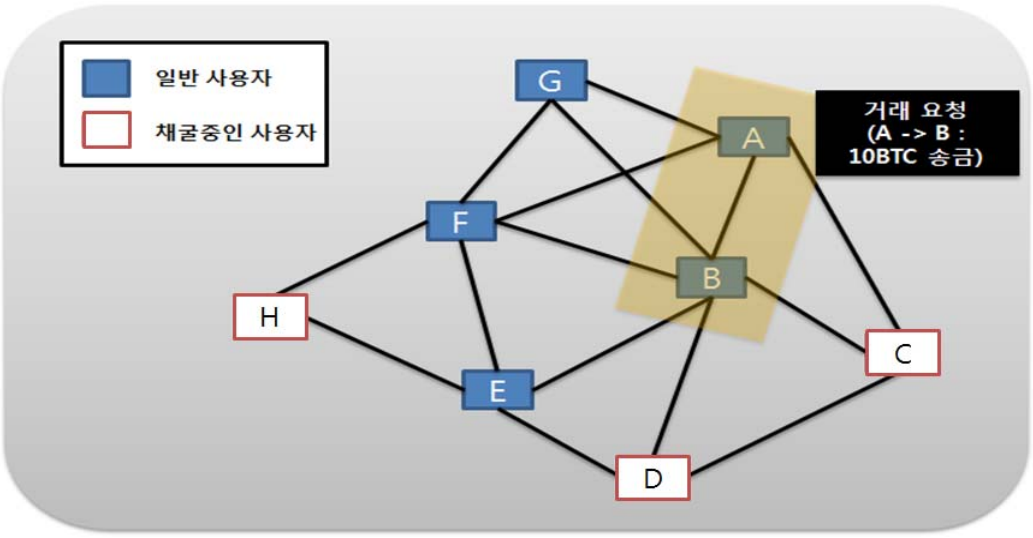
□ 중앙의 권위 및 제 3자의 보증에 의존하지 않고 사용자와 사용자간(Peer to Peer, P2P)의 직접적인 가치 전송의 신뢰성을 보장하는 시스템

□ 블록체인의 구조는 3가지로 설명 가능함

- **분산 합의 시스템** : 보증기관을 통한 에스크로를 보증기관 없이 해결하기 위한 시스템
- **채굴 시스템** : 사용자간 분산 합의 시스템을 운영하는데 필요한 컴퓨팅 자원을 실사용자에게 제공받고 대가로 보상을 주는 시스템
- **거래장부 동기화 시스템** : 모든 사용자가 시스템을 통해 이루어지는 거래내역 전체를 소지할 수 있도록 하는 시스템

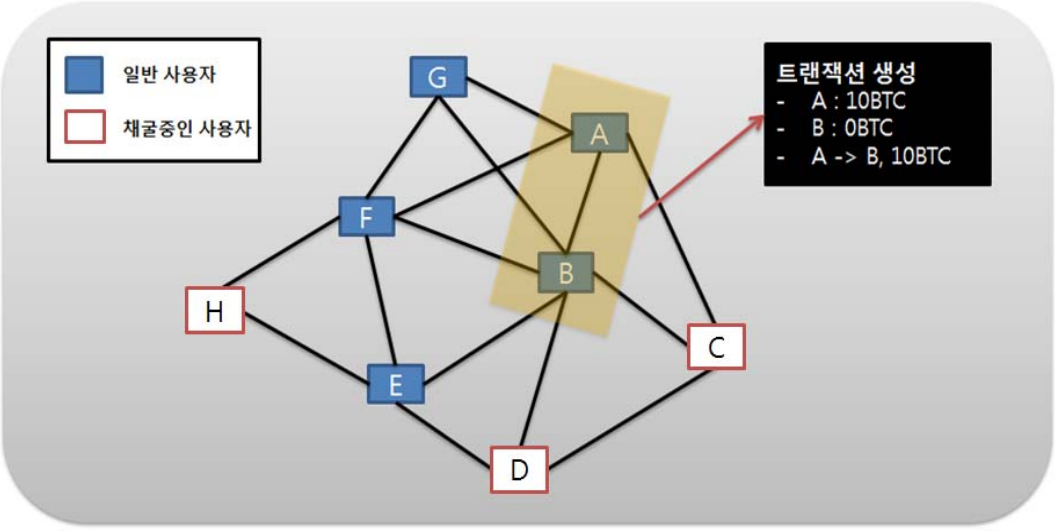
■ 송금 케이스 : A 사용자가 B사용자에게 10BTC를 송금하려 할 때

(1) 송금 요청을 보내는 상황



(2) 거래 요청이 트랜잭션으로 변환(블록화)

- 사용자 간 거래요청이 발생하면, 해당 거래내역은 당사자의 자산정보, 요청된 거래내역 등으로 이루어진 트랜잭션이 되어 복잡한 암호에 의해 블록화 됨

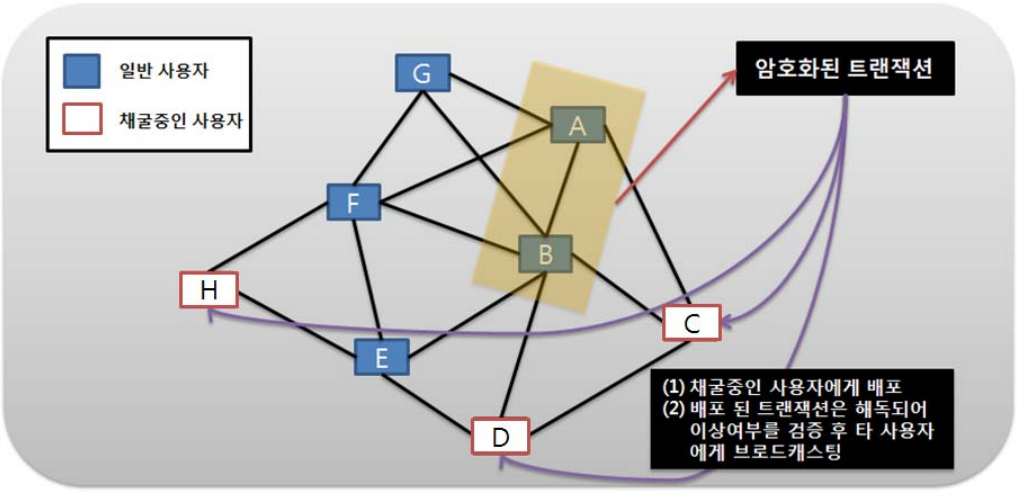


(3) 트랜잭션은 블록화 된 상태로 채굴중인 사용자(세계 전역에 분포된 채굴중인 사용자)에게 전달되고, 블록을 받은 사용자는 해당 거래를 검증

- 채굴은 블록화 된 임의의 트랜잭션 꾸러미를 열기위해 암호를 푸는 과정**<채굴 시스템>**이므로, 각각의 채굴중인 사용자는 자신의 컴퓨팅 파워를 이용해서 암호를 풀고, 거래 요청의 이상여부를 판단해줌(True or False)**<분산 합의 시스템>**
  * 각 사용자의 컴퓨팅 성능에 따라서 기여도가 다름

(ex. 사용자 H의 컴퓨팅 성능이 전체 채굴중인 사용자 컴퓨팅 성능 합의 40% 라면, 해당 컴퓨터가 내리는 검증 결과는 40%만큼의 영향력을 가지게 됨)

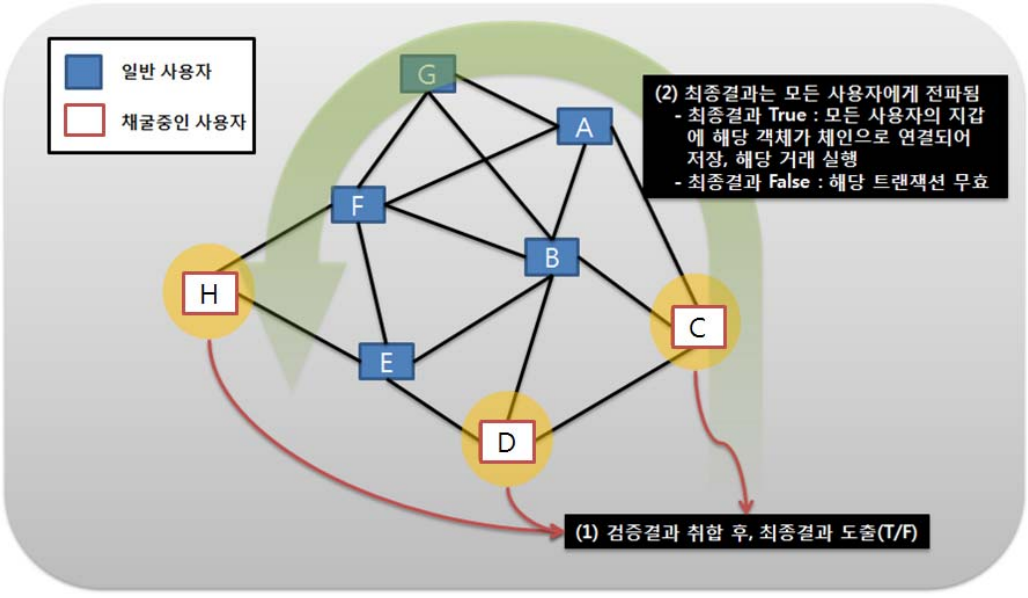
- 각 사용자의 검증결과는 모두 취합되어 과반수에 따라 최종적인 거래적합 여부가 결정 됨



(4) 해당 트랜잭션에 대한 최종 검증 결과를 시스템 사용자 전체에게 전파

- 이상 없는 트랜잭션으로 판정되면 모든 비트코인 사용자의 지갑에 해당 거래 내용이 저장**<거래 장부 동기화>**된 후, 실제 거래가 이루어짐
- 이상 있는 트랜잭션일 시 해당 트랜잭션은 삭제되어 무효 처리됨

* 검증 기여도에 따라 채굴을 수행한 사용자는 일정량의 보상(reward)을 받음



(5) 채굴을 통한 분산합의 시스템은 약 10분 간격으로 수백만 건의 거래 요청을 위의 예시와 같은 절차로 수행하며, 동시 거래량이 점차 많아짐에 따라 채굴을 위해 요구되는 컴퓨팅 파워 또한 증가하고 있음

나. 사용자간 분산 합의 시스템

□ **(필요성)** 3자의 보증이 없는 가치 전송을 위해서는 이를 대체할 수 있는 보증 수단이 필요

□ **(아이디어)** 블록체인에서는 가치 전송을 요청한 당사자를 제외한 불특정 다수에게 현재 요청된 거래에 대한 검증을 맡김

□ **(합의 절차)** 거래에 대한 검증 권한을 갖게 된 사용자 개개인은 해당 거래내역의 정당성을 승인해주고, 다수의 승인결과를 시스템 내에서 종합하여 정당한 거래로 인정하거나 제한함

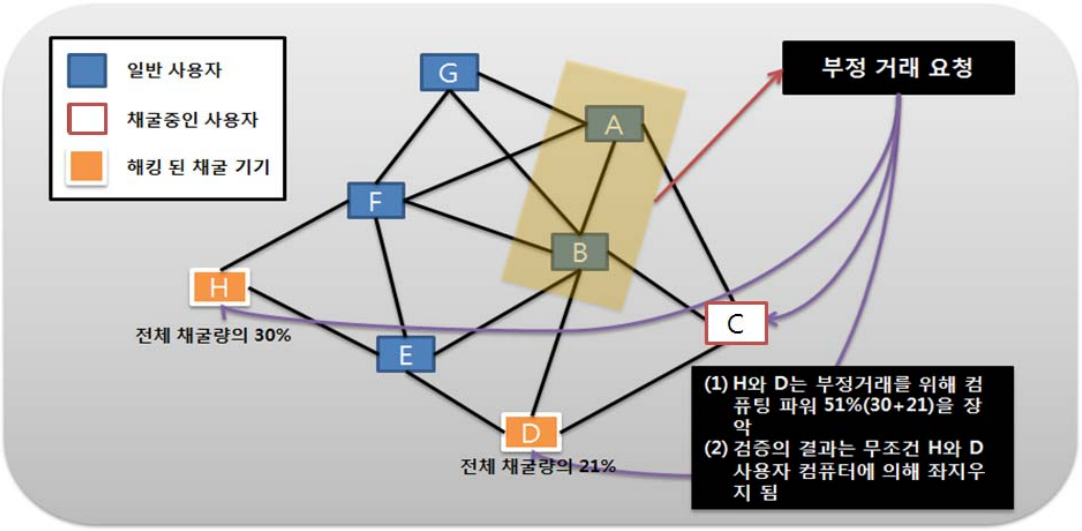
○ 최종 거래로서의 승인결과는 검증 권한을 가진 사용자 전체의 51% 이상의 일치 된 의견을 따르게 되어 있음

○ 부정한 거래 요청을 승인시키기 위해서는 거래에 대한 검증권한을 가질 가능성이 있는 컴퓨터 전체의 51%를 제어해야만 가능함

■ **참고 : 51%의 위협**

(1) 세계 전역의 채굴 중인 컴퓨터 성능 합의 51%이상을 한사람이 점유한다면 이론적으로 부당한 거래를 승인할 수 있음

- 어떠한 트랜잭션이 부정한 거래이나 정상적인 거래로 간주될 수 있는 방법은 블록체인 시스템 내에서 거래의 검증을 맡고 있는 채굴 컴퓨터성능 합의 과반수 일치를 얻어야만 함
- 비트코인의 사용자가 적었을 때는 이와 같은 문제점이 수면위로 드러났으나, 현재는 개인이 소유할 수 있는 컴퓨팅 성능의 실질적 한계로 인해 사실상 불가능하다 볼 수 있음



다. 채굴(Mining)

□ **(정의)** 블록체인에서 거래에 대한 검증은 필수적으로 시스템 내에서 합의 되어야 하며, 채굴은 개인의 컴퓨터를 일정부분 해당 블록체인의 검증에 활용되도록 기여하는 개념임

□ **(검증권한 획득)** 사용자가 개인 컴퓨터를 채굴을 위해 사용하게 되면, 세계 각지에서 채굴을 위해 활성화 된 컴퓨터와 경쟁하여 새로운 거래 내역에 대한 검증권한을 얻음

□ **(검증 절차 및 보상)** 검증권한을 가지게 된 사용자의 컴퓨터는 암호화된 거래 내역을 해독한 후, 네트워크로 연결 된 사용자의 거래장부들과 비교하여 조작 된 거래인지에 대한 확인을 수행하며 보상으로 비트코인을 획득하게 됨

□ **(화폐의 발행)** 사용자는 자신의 실물자산(컴퓨팅 파워)을 제공하고 보상으로 비트코인의 내부자본인 BTC를 받는 구조이며, 보상 개념으로 부여하는 BTC는 결과적으로 화폐의 발행 역할을 대신하고 있음

■ 참고 : 검증(Confirmation)

(1) 빠른 검증

- 레스토랑에서 식사를 하거나, 편의점에서 소액구매를 할 때 거래를 하는 상호간의 즉각적인 가치 교환이 요구됨
- 채굴 절차를 한 번 거쳐 거래 내역에 대해 검증되고 자산이 집행되는데 까지 약 10분이 소요되며 확률적으로 한 거래에 대해 6번 검증이 수행되었을 때(6 Confirmation) 가장 안전한 검증확률을 보장함에 비추어 볼 때, 소액거래에는 적합하지 않음
- 이 때문에, 소액구매에 대해서는 0~1 Confirmation(검증단계를 최소화)을 고려하는 경우가 있으며 이는 소액구매를 가능하게 하는 대신에 다양한 취약점이 생길 수 있음

* 예) 5BTC를 소유한 사용자가 오프라인 매장 두 곳에서 10분 안에 5BTC인 물품을 두 개 구매하고 물품을 수령하면, 검증이 끝난 10분 뒤에는 잔고보다 더 많은 물품을 구매한 것이 되며, 이에 따른 비트코인 사기의 피해 책임소재(손실 된 코인)는 불분명하나, 관련 피해에 대한 이슈는 발생하지 않은 상황임

(2) 느린 검증

- 즉각적인 가치교환이 필요 없는 인터넷 서점, 택배 요청 등의 거래는 결재 요청 이후 충분한 검증 시간이 주어짐
- 빠른 검증에 비해 결재액수가 높지만 신뢰성 측면에서 안전성이 확보되어 있으므로 중복 결재 등의 이슈는 미미한 상황임

라. 거래장부 동기화 시스템

□ **(필요성)** 사용자간 분산합의 시스템의 작동을 위해서는 검증권한을 가진 임의의 사용자들이 거래를 요청한 주체의 최근 거래 내역 및 일련의 정보를 동일하게 가지고 있어야 함

□ **(정보 조작의 내성 효과)** 과거의 거래 내역은 모두 채굴시스템을 통해 과반수 승인을 얻은 신뢰 가능한 정보이므로, 세계의 모든 사용자가 동일한 과거의 거래 내역을 가지고 있다면 특정 사용자의 지갑 내 거래 내역을 조작하더라도 과반 수 승인을 얻기 힘들어짐

□ **(구조)** 세계 전역의 거래 내역 일체는 블록(거래 내용이 담긴 상자)의 형태로 저장된 후, 거래의 시간 순으로 연결되어 사용자 각각의 지갑에 동일하게 저장 됨

- ○ 개인 사용자는 세계의 모든 거래 내역을 가진 지갑을 가지며, 사용자간 분산합의가 완료된 거래내역이 블록의 형태로 추가될 때마다 자동으로 동기화 됨
- ○ 개인 지갑의 용량은 2015년 3월 기준 21GB 선을 돌파한 상황이며, 2009년부터 축적 된 거래 장부라는 것을 감안했을 때, 현재의 저장소 발전 속도로 충분히 수용 가능함

마. 요약

□ 비트코인은 블록체인이란 기술을 활용하여 성공한 최초의 어플리케이션으로서 바라보아야함

□ 블록체인 기술의 핵심 아이디어는 '탈중앙화(Decentralized)'이며 기술을 구성하는 몇 가지 기능(사용자간 분산합의, 채굴, 트랜잭션 동기화)은 이러한 아이디어를 산업에 적용하기 위한 아래의 목적에 기반 하여 만들어짐

- ○ 사용자간 분산합의 : 제 3자의 보증 없이 신뢰성 있는 가치 전송을 보장하기 위함
- ○ 채굴 : 시스템의 자율적 운영보장 및 보상을 통한 초기 사용자의 동기부여
- ○ 거래장부 동기화 : 보안위협에 대한 시스템의 내구성 향상

□ 화폐가 아닌 기술의 시각에서 바라보았을 때, 시스템 활용 방법에 따라서 가치 전송이 필요한 서비스분야의 중앙관리형 시스템을 대체할 수 있음(예 : 클라우드 서비스)

3. 비트코인 2.0 그리고 이더리움(Ethereum)

□ 비트코인의 기능적 한계는 오로지 '내부 자본의 전송' 만을 보장한다는 점임

□ 상업적인 가치를 가지기 위해서는 시스템내의 가치 전송과 실물자산 및 기타 디지털 자산 사이의 자유로운 계약(Contract)이 성립되어야 함

□ 비트코인의 설계 목적은 화폐로서의 신뢰성을 보장하는 순환체계구축이었으므로, 기본적인 내부자본(BTC)의 속성은 내부자본의 양을 표현하는데 그침

가. 비트코인 2.0

□ **(정의)** 비트코인 시스템을 확장하여 개선 된 화폐를 만드려는 노력 또는, 중앙관리형 서비스들의 대안을 제공하려는 일련의 시도를 비트코인의 한 단계 진화한 모습이라는 뜻의 2.0으로 정의함

□ **(스마트 컨트랙트)** 비트코인 2.0 시스템의 필요성을 설명하기 위해 가장 중요한 키워드로서, M2M(Machine to Machine)의 구현을 위한 스마트 컨트랙트(Smart Contract)가 있음

○ 현재 사물을 다루는 행위의 주체는 인간이었으나, 인간이 사물을 제어하는 행위를 일련의 규칙으로 정의하는 방법

○ 각종 규칙은 하드웨어 또는 소프트웨어 내부에 스크립트 언어로 정의할 수 있으며, 미리 정해진(프로그래밍 된) 규칙에 따라 사람의 개입 없이 의도된 방향으로 기기와 기기 사이의 커뮤니케이션, 각종 추천 결과 도출, 기기과 기업간 데이터 교환 등을 지원

- M2M 사례 : 사물인터넷
- M2C 사례 : 금융서비스의 수익률 분석 및 자동화 된 자산 투자
- M2B 사례 : 기업의 ERP와 판매상품(기기)간의 데이터 교환

○ 기기간의 소통이 가능해야 하므로, 모든 기기는 동등한 레벨의 네트워크로 연결되어 있어야 하며 각 기기내부에 정해놓은 규칙의 명세는 동일한 언어로 쓰여져 있어야 함(P2P 네트워크 환경에 적합)

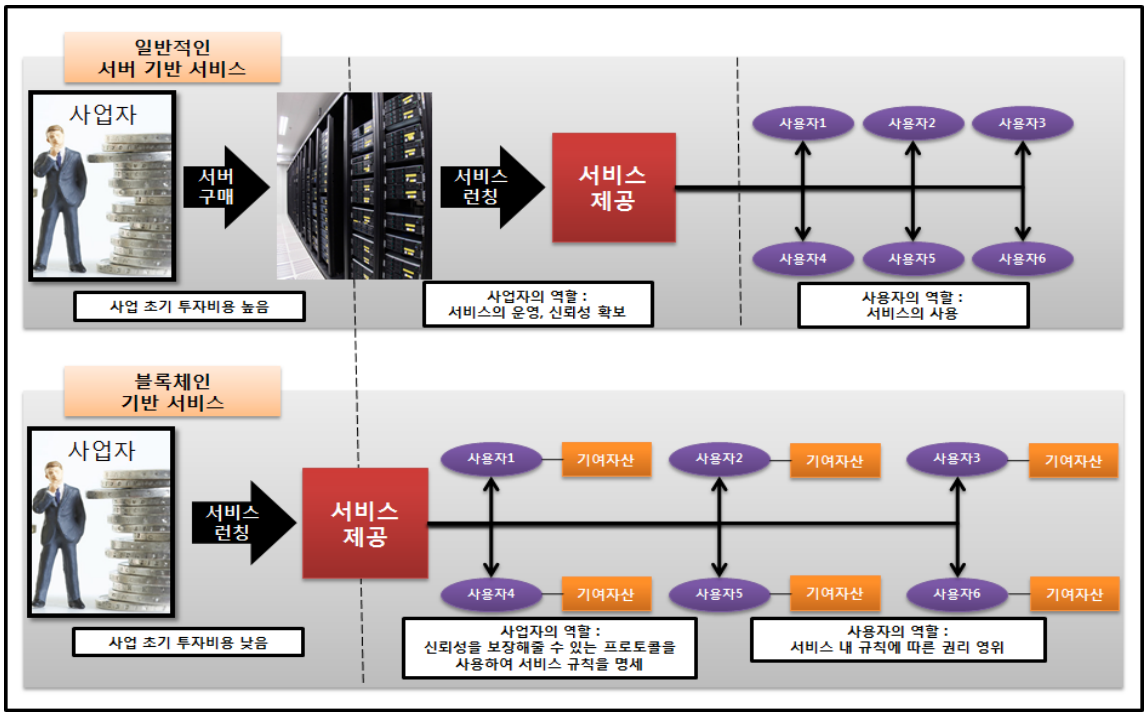
○ 사람은 규칙을 정한 후 관여하지 않고, 거래 및 의사전달의 주체는 기기가 되는 현상으로서 “Decentralized Autonomous Organization(DAO)”라는 용어로 해당 개념을 정의함

□ **(활용 범위)** 비트코인2.0은 화폐의 금융서비스 호환성 강화, 탈중앙화(Decentralize)된 서비스 지원 관점에서 바라볼 수 있음

○ 화폐의 금융서비스 호환성 강화 : 화폐로서의 역할은 동등하게 적용하면서 사이드체인을 활용하여 금융서비스에 필수적으로 필요한 고유한 속성을 부가적으로 지원

- 기존 화폐는 어음, 채권 등의 고유한 특성을 가진 증권의 형태 등으로 즉각적인 전환이 용이함
- 비트코인은 법정화폐로 인정되지 않기 때문에 다른 형태의 자산과 거래하기 위해서 환전소를 통한 기존 자산으로의 전환이 선행되어야만 하므로, 다른 형태의 자산과의 사이드체인 형성을 통해 가치교환 절차를 간소화 하려는 시도가 이루어지는 추세임
- 사이드체인의 도입은 비트코인의 일반적인 금융서비스를 위한 절차를 간소화 시킬 수 있기 때문에, 일반 화폐의 기능에 좀 더 근접하기 위한 시도로 해석 가능함

그림 7 기존 서버기반 서비스와 블록체인 기반 2.0 서비스의 차이점



자료 : 소프트웨어정책연구소

○ 탈중앙화 된 서비스 지원[7] : 중앙에서 서버제어 및 DB수집을 수행하는 형태를 기반으로 한 서비스[8]의 중앙 서버를 없애고, 서버가 수행했던 업무들을 서비스를 사용하는 사람들의 기기가 분담하여 처리하도록 변경함

- 이러한 시스템은 사용자가 서비스를 사용하기 위해 저장소 또는 컴퓨팅 파워의 일부를 기여하도록 구조화 되어 있음
- 중앙서버에서 수행했던 역할은 사용자들이 분산하여 맡게 되고 각 사용자가 그 역할에 얼마나 기여하는지에 따라 보상으로 시스템 사용을 위한 차등 권한을 부여

※ 비트코인이 채굴을 통해 검증을 확보한 것과는 다르게, 해당 서비스는 서비스 수행을 위한 자원을 확보

- 화폐로서의 역할을 했던 시스템 내 자산이 해당 시스템 내에서는 특정 서비스를 이용할 수 있는 권리로서 작용

나. 이더리움의 등장

□ 이더리움(Ethereum)은 비탈릭 부테린(Vitalik Buterin)[9]이 창립한 회사의 명칭이자 그의 아이디어를 구현한 웹 프레임워크의 이름임

○ 지난 4월, 제한적인 기능만을 제공하는 1차 소스코드 공개를 단행하였고, 이후에 총 2번에 걸쳐 제한 된 기능을 개방하였음

○ 8월 초 계획되었던 전체 기능을 포괄하는 정식 서비스가 오픈[10]

□ 프로그래밍 가능한 블록체인(Programmable Block-chain)

○ **(목적)** 이더리움의 기본 철학은 범용성 있는 블록체인기반 환경조성 지원 프레임워크를 제공하는 것에 있음

---

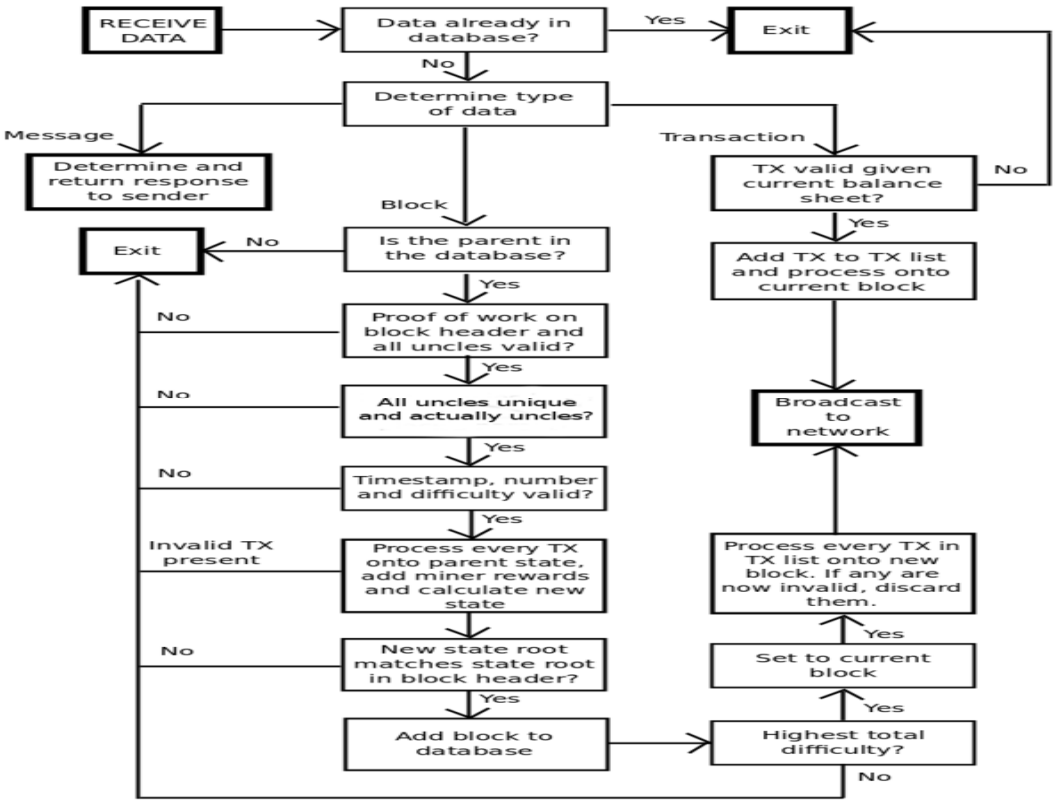
7) 해당 측면에서 바라본 2.0 시스템은 화폐개념을 버리고 내재된 기술인 블록체인을 활용한다는 점에 집중하기 때문에 그런 이유에서 해당 업계는 “블록체인 2.0”이라는 표현을 사용함

8) IoT 스마트홈 시스템, 인터넷 도메인, 인터넷 에스크로 서비스 등

9) Vitalik Buterin : 20세 캐나다인으로서, 비트코인 커뮤니티에서 활동하던 중 탈중앙화된 인터넷 프로토콜에 대한 아이디어를 고안해 내었고, 이 아이디어를 토대로 제시한 이더리움(Ethereum)의 개발 계획이 주목을 받아, 신기술 분야의 노벨상으로 불리는 “World Technology Award”의 IT 소프트웨어 수상자로 뽑힘

10) https://blog.ethereum.org/2015/07/27/final-steps/

그림 8 이더리움 클라이언트의 범용 P2P 프로토콜(ethereum.org)



출처 : ethereum.org

○ 비트코인의 블록체인을 활용하기 위한 기존의 방식은 앞서 설명한 사이드체인 사용 또는 비트코인 소스코드를 분석하여 수정해야만 가능했음

○ 특히, 금융서비스 관점이 아닌 탈중앙화 서비스 지원이 목적인 경우, 비트코인 소스코드의 상당량을 변화시켜야하기 때문에 매우 비효율적임

○ **(특징)** 이더리움은 이 점에 착안하여 기본적인 블록체인을 제공하고, 여기에 추가로 메시지 송수신과 저장소 기능을 지원하는 범용 블록체인 환경을 제안함

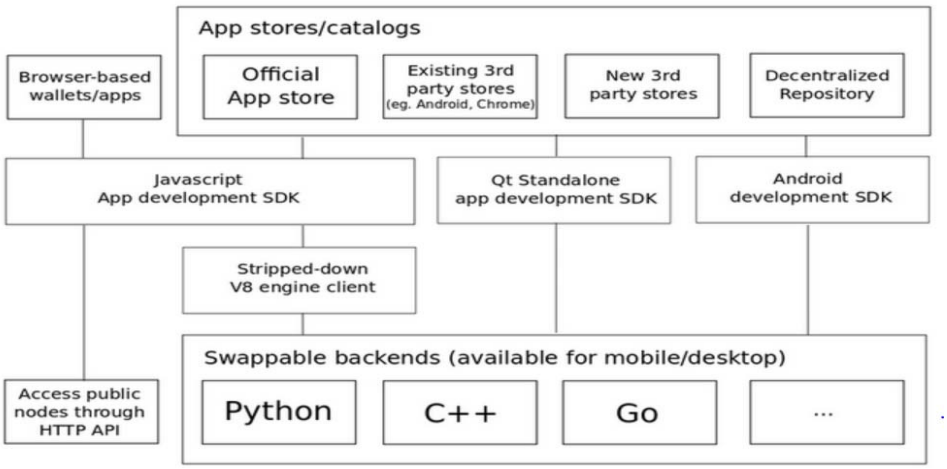
○ 기본적으로 제공되는 환경 하에 특정 서비스 개발이 목적인 이용자는 이더리움에서 제공하는 API(Application Programming Interface)를 활용하여 사용자에 친숙한 프로그래밍 언어로 하여금 서비스 모델을 구축하고 이를 사용할 수 있도록 지원

○ JVM(Java Virtual Machine)과 비슷한 원리로 EVM(Ethereum Vitual Machine)을 지원

□ 분산어플리케이션(Dapps)

○ **(정의)** 이더리움의 EVM위에서 동작하는 분산환경기반 응용프로그램을 지칭함

그림 9 이더리움 Dapp 생태계 다이어그램(ethereumbuilders)



출처 : ethereumbuilders(github.com)

○ 이더리움 내 블록체인의 내부자본 이더(ETH)의 정의에 따라서 자유도가 높은 서비스 개발을 목적으로 함

○ 비트코인과 파일 공유 시스템 비트토렌트가 분산어플리케이션의 대표적 예임

다. 이더리움 기반 사물인터넷 구현 계획 - ADEPT

□ 블록체인 기술을 통한 IBM의 사물인터넷 통합 플랫폼 계획으로서 An IoT Practitioner Perspective(ADEPT)로 통칭함

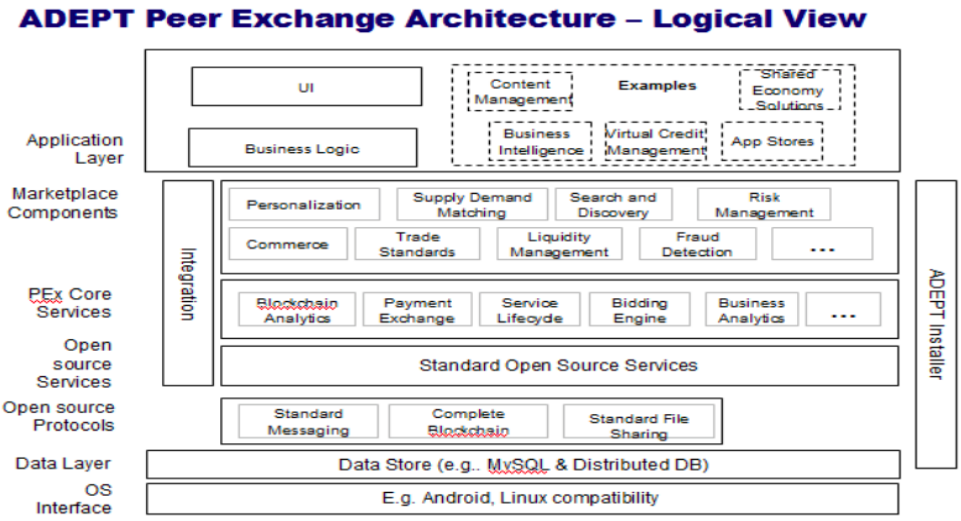
□ ADEPT의 논리적 구조는 크게 3가지로 분류 됨

○ 시스템 계층 : 블록체인 기술 및 분산 환경 구성에 필요한 메세징, 저장소 개념을 포함한 환경 구성 계층

○ 분석 계층 : 시스템 계층과 응용 계층 사이의 각종 데이터 수집 및 분석과 관련한 다양한 API를 제공할 것으로 예측됨

○ 응용 계층 : UI, 사업구조등을 정의하며 기계 자동화, 신용 관리, 자산 공유 등의 직접적인 응용을 지원

그림 10 IBM-Samsung ADEPT 아키텍처



출처 : IBM White Paper - ADEPT

□ ADEPT의 구현을 위한 프로토콜로서 IBM은 현재 존재하는 P2P기반 솔루션을 활용하려는 계획임

○ TeleHash : 분산 메시지 프로토콜

○ BitTorrent : 분산 파일 공유

○ Ethereum : 블록체인 환경 및 계약 시스템[11]을 위한 완전튜링언어(프로그래밍 언어) 제공 플랫폼

□ ADEPT - B2C 사례

○ 소모품 추가 주문 자동화

- 기기를 사용하는데 있어 소모품이 존재하는 경우, 기기에 내장되어 있는 계약(Contract)에 따라서 소모품의 주문 필요성을 체크하여 오프라인 공급자에게 주문 요청
- 공급자는 타블렛과 같은 기기를 통해 각 주문을 수신하고, 대금을 지급 받은 뒤 해당 소모품을 발송
- 이러한 예는 하드웨어 내 계약이 반자동화 되어 수요자와 공급자의 편의성을 향상시키는 목적으로 활용 가능함

11) 계약(Contract) : 인간 또는 기기가 어떠한 조건하에 하는 행동(Action)에 대한 명세를 계약이라 칭하며, 이더리움은 기기간의 계약을 사람이 정할 수 있게 만들어서 사람이 관여해야만 했던 일련의 행동을 각각의 기기가 자동으로 수행하는 IoT의 개념을 수행할 수 있게 함

○ 기기 수리 자동화 서비스

- ADEPT가 적용 된 모든 기기는 고유한 ID를 보유하고 있으며, 이 ID는 ADEPT 호환 기기 간 형성되어 있는 블록체인 네트워크에 등록 됨
- 특정 기기의 하드웨어 문제가 발생 시, 블록체인 네트워크 내부에 소속 된 다른 기기를 통해 관련 문제가 식별 되며, 문제해결을 위한 서비스 업체를 미리 설정해 둔 계약내용에 의해 자동으로 선별하여 AS 절차(서비스 업체에 고장내역 송신, 관련 AS를 위한 단가 수신 및 사용자에게 포워딩 등)를 자동으로 수행

○ 물리적 자원 관리(전력 관리)

- 블록체인 네트워크로 연결 된 ADEPT호환 기기들에 대한 전력 소모를 체크하여, 설정한 계약 내용에 따라서 전력의 유동적인 공급 제어를 지원함
- 계약의 정의에 따라, 특정 주기 동안의 전력 소모의 평균량을 계산하여 이에 맞추어 적정 전력량의 기준을 변화하는 방법을 통해 스마트 그리드(Smart Grid)를 실현 가능함

라. 요약

□ 비트코인 2.0은 화폐로서의 속성에서 확장하여 내부의 블록체인 기술에 주안점을 두어 파생되는 서비스를 가능하게 만들자는 아이디어로부터 시작함

□ 현재 해외의 서비스 사례에 기반 하여 두 가지 유형의 서비스로서의 발전이 진행 중임

○ 화폐의 금융서비스 호환성 강화
○ 탈중앙화 된 서비스 지원

□ 이더리움은 C++, JAVA와 같이 블록체인 기반 SW개발을 위한 환경을 제공하기 때문에, 비트코인2.0에 해당하는 잠재적인 서비스 창출 활성화에 큰 기여를 할 것으로 보임

□ 한편, IBM과 삼성은 P2P 아키텍처를 통한 사물인터넷 구현을 위해 이더리움 기반 플랫폼인 ADEPT를 제안함

□ 국내 기업에서도 블록체인 기반 플랫폼과 관련한 해외 기업과의 협업이 추진되는 상황에 비추어 볼 때, 국내 산업에 관련 기술이 유입될 시 발생 가능한 몇 가지 유형 별 시나리오를 살펴 볼 필요가 있음

4. 산업적 파급효과

가. 블록체인 기술 유입 유형 별 시나리오

□ 비트코인2.0 플랫폼이 국내에 출현할시, 예상되는 시나리오는 세 가지로 추정해 볼 수 있음

○ **(대기업 중심)** 중앙관리형 서비스의 보완제 역할을 수행하는 IoT기술 개선을 목적으로 한 플랫폼 형태로의 유입

- 기존 데이터센터 및 중앙관리형 서비스를 운용하던 거대 기업은 쉽게 기존 중앙관리형 인프라를 포기하지 않을 것
- 중앙관리형 시스템은 빅데이터의 수집에 이점이 있기 때문에, 블록체인 기술은 주로 “가치가 없는” 데이터를 발생시키는 단순 클라이언트를 중심으로 적용 될 가능성이 큼
- IBM 및 삼성이 협업 추진하는 P2P플랫폼인 ADEPT 또한 구체적인 형태가 공개 되지 않았으나, 시스템 내부 구조는 블록체인 기반의 P2P 형태를 취하고, 2차 서비스들에 대해서는 데이터 수집이 용이한 형태를 계승할 것으로 전망됨
- 해당 경로를 통해 서비스 유입 시, IoT를 효과적으로 구현할 수 있는 기술로서 기존 인프라를 위협하지 않는 차원에서의 자연스러운 보완제 역할을 수행할 것

○ **(스타트업 중심)** 비트코인 커뮤니티 등을 통해 활동하는 IT스타트업에 의한 도전적인 서비스 런칭과 함께, 이더리움 호환 플랫폼으로서의 IoT기기 출현

- 서비스 도입의 낮은 장벽을 이용한 이더리움 호환 IoT기기 또는 웹 컨텐츠의 유입

- 중앙관리 체계 구축에 소모되는 초기 투자비용을 비트코인2.0 기술을 통해 극복할 수 있기 때문에, 인프라 형성 초기 단계를 전략적으로 극복하는 스타트업이 출현할 것

- 서비스 도입 이후 안정기까지 거대기업과의 경쟁이 불가피 할 것이기 때문에 고객확보 및 자사 비트코인2.0 기술 적용의 타당성을 효과적으로 설파하는 것이 중요한 요소가 될 것임

- 국내 유입의 시작을 이더리움을 위시한 해외 플랫폼을 통해 시작하게 될 경우, 지속적인 호환성 유지를 위해 국내에서 높은 점유율을 차지하고 있는 Microsoft의 Windows OS처럼 응용기술의 모든 컨트랙트에 대한 환경 구속력이 생길 여지가 있음

○ **(해외서비스 중심)** 국내 유입의 지연으로 인한 검증 된 해외서비스 국내 잠식 가능성

- 해외 기업의 성장 이후, 국내 산업 생태계에 위협으로 작용하였을 때 관련 이슈의 등장 및 뒤늦은 정책적 대처로 이어질 가능성이 있음

- 국내의 간편결제시장 형성과 유사하게 내수시장에 집중한 토종 서비스가 연이어 등장할 것으로 전망됨

- 이는 글로벌한 서비스 노하우 및 고객 확보 등에서 스스로 제한을 설정하는 일이므로, 장기적으로도 규모의 경제 측면에서 경쟁력을 상실하게 될 것

나. SWOT 분석

유입 경로 / SWOT	국내 대기업 중심	국내 스타트업 중심	해외 기업 중심
강 점	• 국내 시장 장악 용이 • 자본력을 통한 공격적인 마케팅 • 기존 플랫폼의 확보된 고객을 이용 가능함 • 해외 블록체인 플랫폼에 독립된 기술 경쟁력을 가질 수 있음	• 독창적 아이디어 • 서비스 형태에 집중 • 기존 중앙관리형 시스템에 반하는 모든 서비스를 지원하는 어플리케이션 제안이 가능	• 산업 적용이 완료된 완성도 높은 서비스 • 고객 수요를 만족시키는 다양한 호환기기 지원 • 자연스러운 글로벌 서비스의 체험이 가능
약 점	• 자사 플랫폼 위주의 호환성으로 인한 독점현상 • 중앙관리형 시스템의 수익모델과의 공존이 강제됨	• 초기 고객 유치의 어려움 • 대기업의 유사 서비스 런칭 시, 경쟁력 열세 • 해외 종속적 플랫폼 운영을 통한 원천 기술 특허의 어려움 • 금융 서비스 진출이 다소 힘듦	• 글로벌 경쟁력 우위에 있으나 국내 시장에 특화된 서비스 제공이 어려움
기회요인	• 발빠른 트랜드 파악을 통한 해외 기업과의 기술적 제휴 • 관련 특허 및 표준의 부재	• 국내 핀테크 도입에 의한 전자결재 법규의 완화 추세 • 비트코인2.0 플랫폼의 낮은 초기 투자 비용	• 비트코인2.0의 발현지로서의 기술 및 서비스 선도 • 가격 경쟁력
위협요인	• 실험적 시도에 보수적 • 기존 인프라의 성공적 안착 • 기업 특성상 수익모델의 당위성 증명 필요	• 국내의 블록체인 기술 인지도 부족	• 해외 기술 독점현상 우려에 따른 국내 규제 가능성

다. 기존 산업이 받을 영향

□ 사물인터넷 - 스마트 컨트랙트(Smart Contract)

○ 스마트 기기 간 상호 작용의 자동화를 위해서는 중앙 관리를 담당하는 서버가 없이 각각의 기기가 설정해 놓은 규칙(Rule)에 따라서 사람의 개입 없이 각종 업무처리가 가능해야함

※ 예 : 자판기 재고를 기계가 스스로 판단하여 인터넷을 통해 발주처리함으로써, 오프라인에서의 사람의 개입(관리)을 최소화함)

○ 모든 IT기기가 각각의 정해진 규칙(계약)에 따라서 허용된 범위내의 타 기기와 통신하며 규칙을 적용하고 처리하는 형태로서 사람은 이러한 규칙을 숙지하고 있되 개입할 필요가 없어짐

○ 현재 기기 판매자 및 동일 브랜드에 국한 되어 서비스 되는 사물인터넷 가정용 임베디드 플랫폼들은 점차 사라지고, 블록체인 기반의 신뢰성이 보장 된 자동화 시스템으로 대체 될 것임

○ 또한, 현행 서비스 되고 있던 오프라인 편의시설에 다양한 컨트랙트를 내장하여 시설 관리 인력 수요가 감소될 것으로 전망

○ 이는 계약의 구현을 통한 자동화 아이디어를 가진 스타트업의 양산으로 이어지는 반면, 잠정적으로 2차 노동인력의 감소 이슈에 대한 우려가 있음

□ 금융 거래의 자동화 - 스마트 에셋(Smart Asset)[12)]

○ 블록체인을 활용한 보안성이 높은 자산 거래 서비스는 이미 해외에서 가장 주목받는 비트코인 2.0의 활용 유형으로 분류됨

○ 주식 거래 또한 스마트 컨트랙트의 개념을 기반으로 서로 다른 자산과 자산사이의 계약으로 정의될 수 있으며, 사용자가 임의로 설정한 특정 규칙에 의거하여 자산의 자동화된 거래를 가능하게 함

○ 은행의 펀드 매니저에 의한 자산관리보다 자산의 투명성이 높아지며 자산의 보안성이 강화되는 효과를 가짐

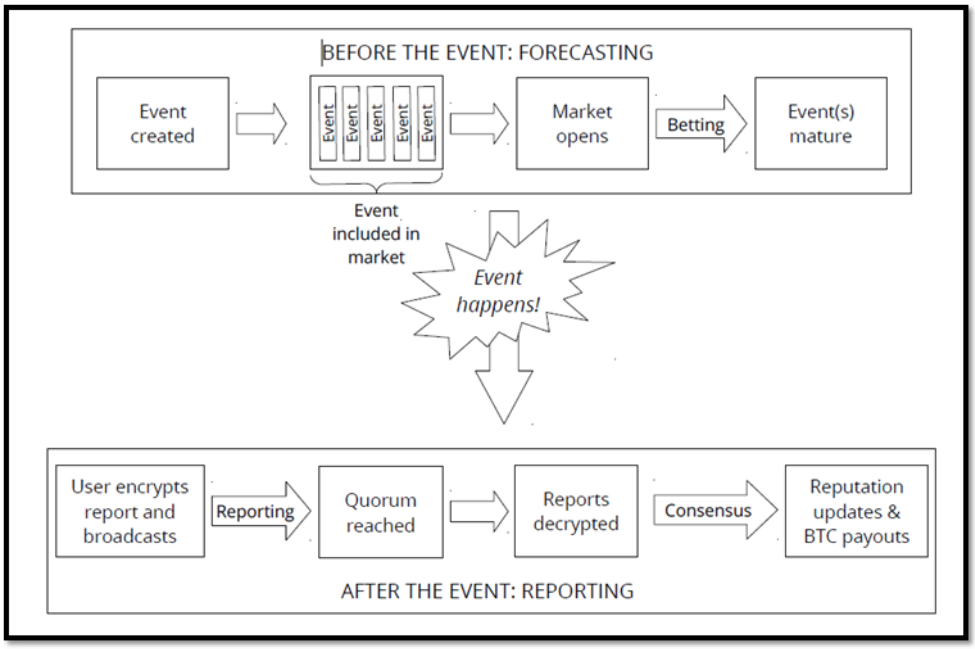
○ 자산 거래 서비스는 현재 국내의 핀테크 규제 완화가 소극적임을 볼 때 쉽게 적용되기는 힘들 것으로 전망되며, 이에 따른 금융 당국과의 마찰이 예상됨

○ 현재로서는 해외의 성공적인 사례가 등장한 이후, 점진적으로 벤치마킹 될 가능성이 높음

12) 스마트 에셋(Smart Asset) : 기존의 자산관리의 주체가 사람인 것에 착안하여, 각각의 자산관리 의도를 계약화 하여 SW에 내장함으로서 자동화 된 자산관리를 지원하려는 시도

□ 미래에 대한 정확한 예측 - 예측시장(Prediction Market)

그림 11 블록체인 기반 예측시장 아웃라인(augur.link)



출처 : augur.link

○ 미래의 사건을 예측하기 위해서 흔히 사용되는 방법으로서 앙케이트 결과 종합을 통한 다수결 예측, 히스토리 분석, 델파이 기법 등이 있음

○ 비트코인 2.0으로 구현 가능한 예측시장의 원리는 일종의 '펀딩'으로 해석 가능함

○ 참여자가 일정 가상자산을 시스템에 펀딩한 후, 자신의 자산을 잃지 않는 방향으로 특정 예측을 하여 예측 정확성을 높임

○ 블록체인 기반 예측시장은 2015년 말 정식 런칭 될 Augur 프로젝트가 가장 주목받고 있으며, 예측 정확도와 관련해서는 정식 런칭 이후 수집되는 적중률을 토대로 기존 예측방법들과의 비교가 가능할 것으로 예상 됨

○ 이러한 서비스는 각각의 예측에 참여할 사용자가 확보되어야만 성립하기 때문에, 비트코인의 사례에서 우려되던 시스템 악용사례나 규제의 위험이 없어 신뢰성이 입증된다면 국내에 쉽게 적용 될 것으로 사료됨

5. 결론 및 시사점

□ 비트코인 2.0은 사물인터넷을 실현하기 위한 필수적인 기술

○ 비트코인 2.0의 스마트 컨트랙트는 기기 간 통신에 있어 중요한 보안성 및 신뢰성 이슈를 분산합의 시스템을 통해 해결함으로써, IoT기기의 금융 자동화 처리 등을 지원하는데 있어 기술적 기반으로 활용 가능함

○ 개인정보 유출, 해킹 등으로 제 3자 인증기관 시스템에 대한 신뢰성 저하가 이슈인 가운데, P2P를 기반으로 하여 개인정보보호 문제에 강력한 내성을 지니는 기술로서 현존하는 보안문제의 해결방안이 될 것으로 전망됨

□ 데이터 독점에 반기를 드는 통제 없는 시스템의 출현

○ 개인정보 유출의 이면에는 개인정보를 수집 및 관리하는 통제기관이 있음

○ 블록체인 기술은 거래에 대한 보증을 대가로 개인정보 데이터를 수집하지 않기 때문에, 각 산업의 독점권을 향유하는 기업을 대상으로 중소기업이 경쟁할 수 있는 하나의 강점으로 활용 될 여지가 있음

○ 반면에 기존 인프라의 이점을 누리던 기업 입장에서는 블록체인 기술 기반 서비스에 큰 매력을 느끼지 못할 것으로 예상됨

□ 비트코인 2.0 기술은 다양한 혁신을 가져다 줄 수 있으나, 사회적인 부작용을 야기할 수 있다는 점에서 도입에 면밀한 검토가 필요함

○ 비트코인 2.0과 같은 신기술의 도입은 창조적 혁신을 위한 인프라 조성에 유용한 촉매제로 활용 될 수 있을 것으로 보이며, 어떤 형태로 해당 기술을 활용하는 것이 사회적 비용을 최소화함과 동시에 국내 산업에 큰 반향을 일게 만들 수 있을 지에 관하여 적극 검토할 필요가 있음

○ 한편, 다양한 계약의 설정을 통한 비윤리적 서비스 제공*, 자산 세탁 등은 개인정보 보호의 이면에서 불법적인 수단으로서 작용할 가능성이 있기 때문에 해당 문제에 대한 사전 대비가 필요함

※ 타인의 IoT기기 개조 및 해킹을 통한 익명의 마약거래, 성매매, 인트라네트워크 내 P2P 불법자료 공유 등

[참고문헌]

국내문헌

[1] 지디넷코리아. (2014.9.15.). “IoT에 비트코인 아키텍처 넣자”
[2] OrganicMediaLab. (2014.1.11.). 비트코인 채굴과 선순환 구조 (Virtuous Cycle of Bitcoin Mining)

국외문헌

[1] O’ reilly. (2015.1.22.). Blockchain : blueprint for a new economy, Melanie Swan
[2] G. Wood. (2014). ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER FINAL DRAFT, GitHub.com
[3] V. Buterin. (2014). Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform, GitHub.com
[4] IBM, SAMSUNG. (2015) ADEPT: An IoT Practitioner Perspective
[5] A. Back, M. Corallo. (2014.10.22.). Enabling Blockchain Innovations with Pegged Sidechains, www.blockstream.com
[6] http://bitcoin.meetup.com/
[7] V. Buterin. (2014.5.6.). DAOs, DACs, DAs and More: An Incomplete Terminology Guide

주 의

1. 이 보고서는 소프트웨어정책연구소에서 수행한 연구보고서입니다.
2. 이 보고서의 내용을 발표할 때에는 반드시 소프트웨어정책연구소에서 수행한 연구결과임을 밝혀야 합니다.

OPEN 공공누리 출처표시 상업용금지 변경금지 공공저작물 자유이용허락

[소프트웨어정책연구소]에 의해 작성된 **[SPRI 보고서]**는 공공저작물 자유이용허락 표시기준 제 4유형**(출처표시-상업적이용금지-변경금지)**에 따라 이용할 수 있습니다.
(출처를 밝히면 자유로운 이용이 가능하지만, 영리목적으로 이용할 수 없고, 변경 없이 그대로 이용해야 합니다.)