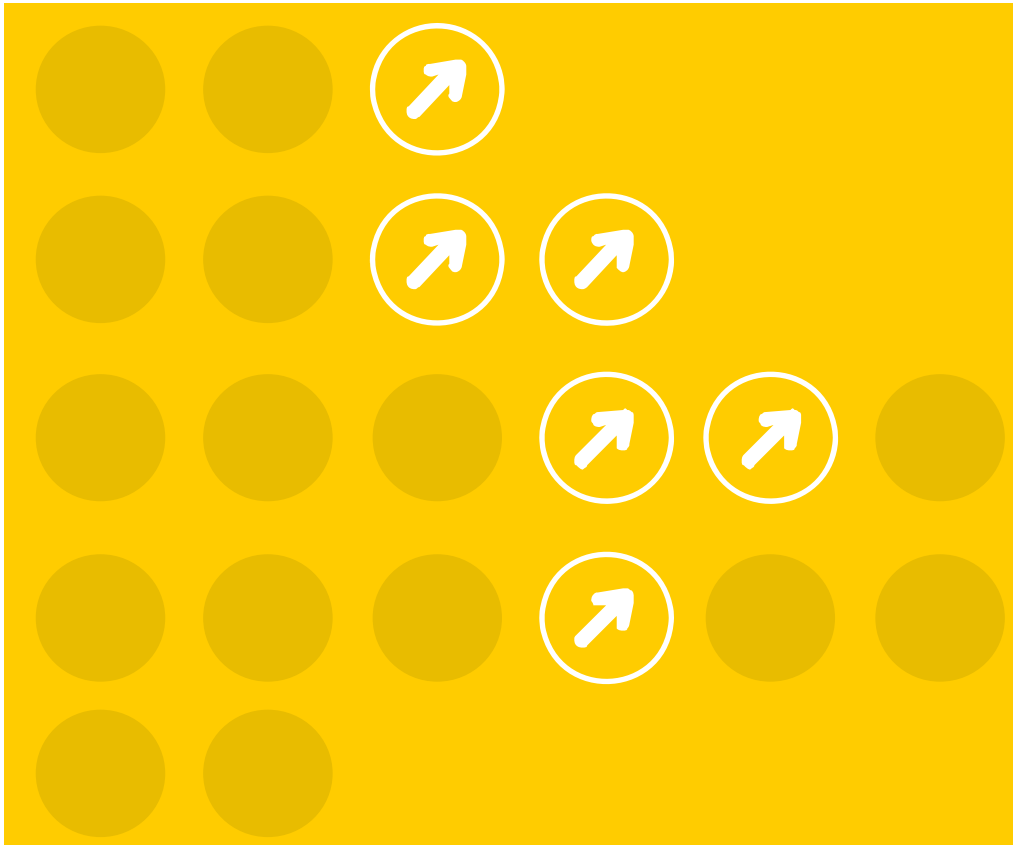
블록체인이 자본시장에 미칠 영향



서강대학교, 경영대학

이군희

Agenda

1. 비잔틴 장군 문제의 해결
2. 블록체인의 이해
3. 비잔틴 장군 문제 해결의 의미
4. 글로벌 자본시장의 블록체인 활용
5. 국내 자본시장의 블록체인 활용
6. 법제적 과제

블록체인: 비잔틴 장군 문제의 해결 !!





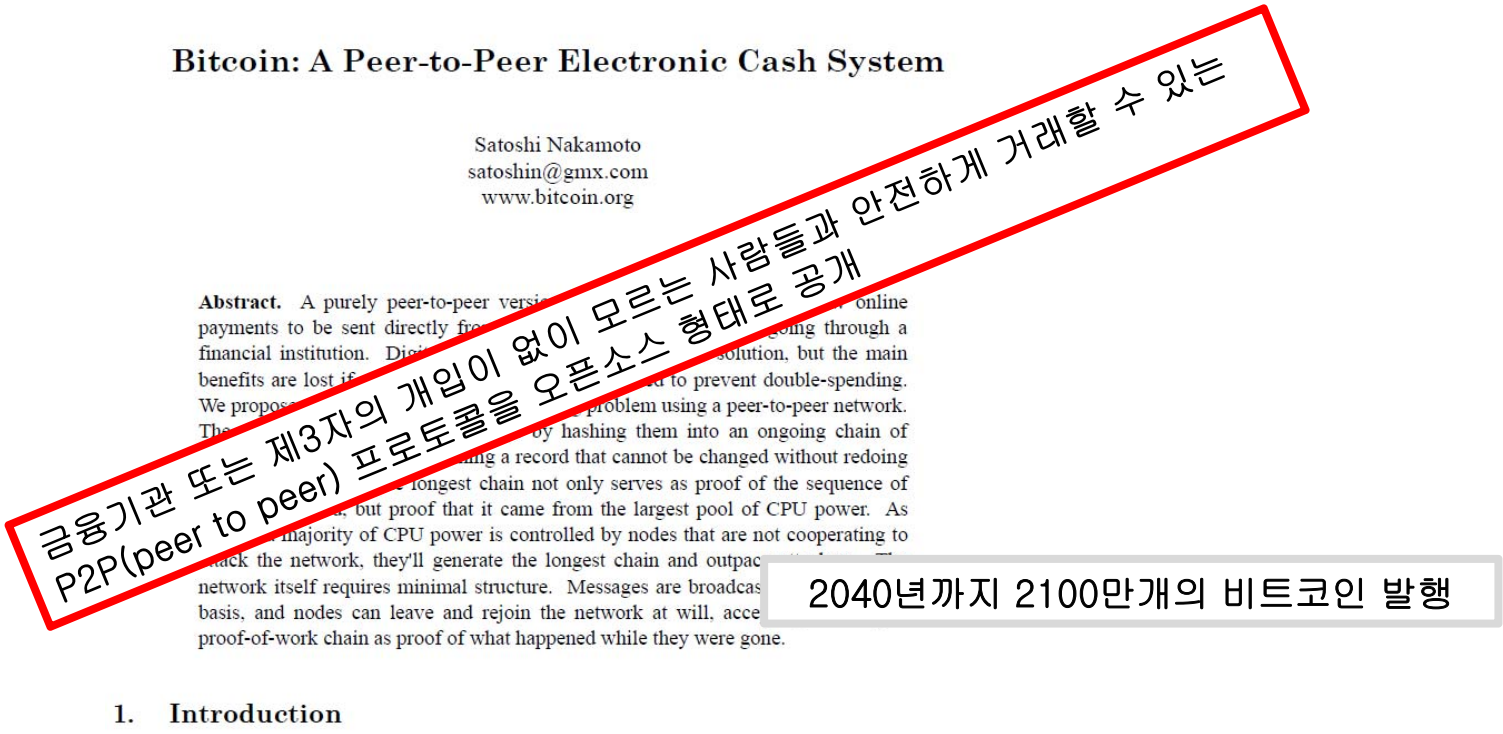






비잔틴 장군 문제의 해결

- 2008년 10월 사토시 나카모토라는 가명의 개발자(해커)가 블록체인 기술을 기반 분산원장 개념을 설명하면서 비잔틴 장군 문제를 해결



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer versi… online payments to be sent directly fr… going through a financial institution. Digi… solution, but the main benefits are lost if… d to prevent double-spending. We propos… problem using a peer-to-peer network. The… by hashing them into an ongoing chain of …ing a record that cannot be changed without redoing …longest chain not only serves as proof of the sequence of …, but proof that it came from the largest pool of CPU power. As …majority of CPU power is controlled by nodes that are not cooperating to …ack the network, they'll generate the longest chain and outpac… network itself requires minimal structure. Messages are broadcas… basis, and nodes can leave and rejoin the network at will, acce… proof-of-work chain as proof of what happened while they were gone.

금융기관 또는 제3자의 개입이 없이 모르는 사람들과 안전하게 거래할 수 있는 P2P(peer to peer) 프로토콜을 오픈소스 형태로 공개

2040년까지 2100만개의 비트코인 발행

1. Introduction

2009년 1월 3일, 비트코인 서비스 시작, 사토시 나카모토가 첫 채굴을 통해 50 BTC 얻음.
닉네임 New Liberty Standard를 사용하는 마이너가 비트코인의 거래 환율을 $1=1309.03BTC로 최초 공시
2010년 8월 6일, 비트코인 프로토콜 상의 보안 문제 발견: 8월15일에 악용되어, 1840억개 비트코인이 생성
➔ 이 문제는 수 시간 내에 해결되었으며 해당 비트코인 블록은 자동으로 제거되고, 프로그램이 수정됨.

글로벌 금융권에서의 블록체인 활용 현황

- 금융권에서 바라보는 블록체인의 시각

  - 분산원장 형태로 활용되고 있으며,
  - 개인 간 네트워크에 분산관리를 통하여
  - 높은 보안성과 낮은 설치 및 유지비용이 장점이라고 판단하고 있음.

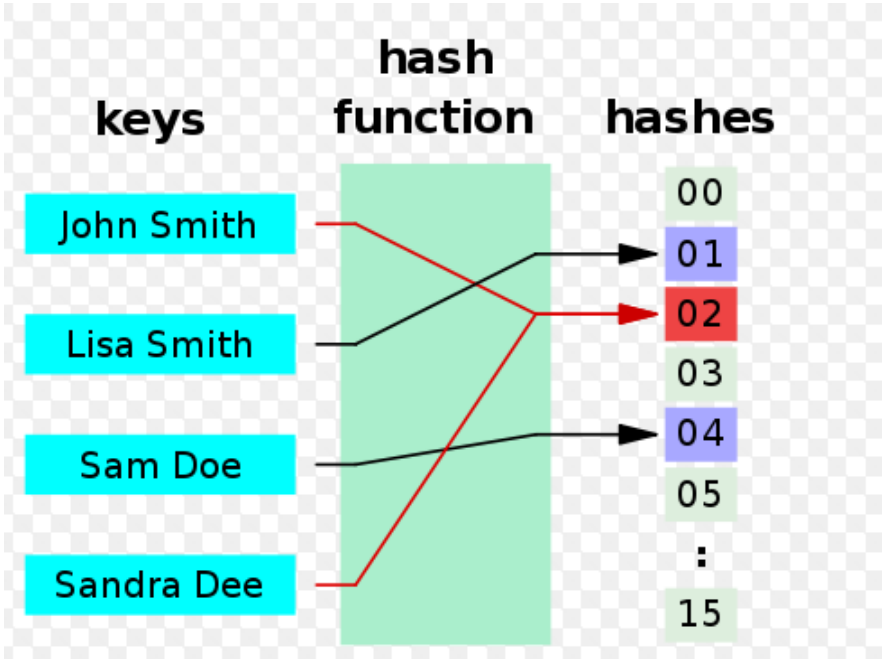
  “블록체인은 거래를 보다 신속하게 처리하고, 시장 운영 비용을 획기적으로 절감하며, 강력한 보안성을 바탕으로 원장에 대한 신뢰성을 높일 수 있다는 등의 강점을 보유한 기술이다.”

  - 정말로? 실효성은? (극복할 문제가 많이 남아 있음)

    법적 제도적 환경, IT자원 관리, 거래 처리 능력, 속도, 비용, 보안

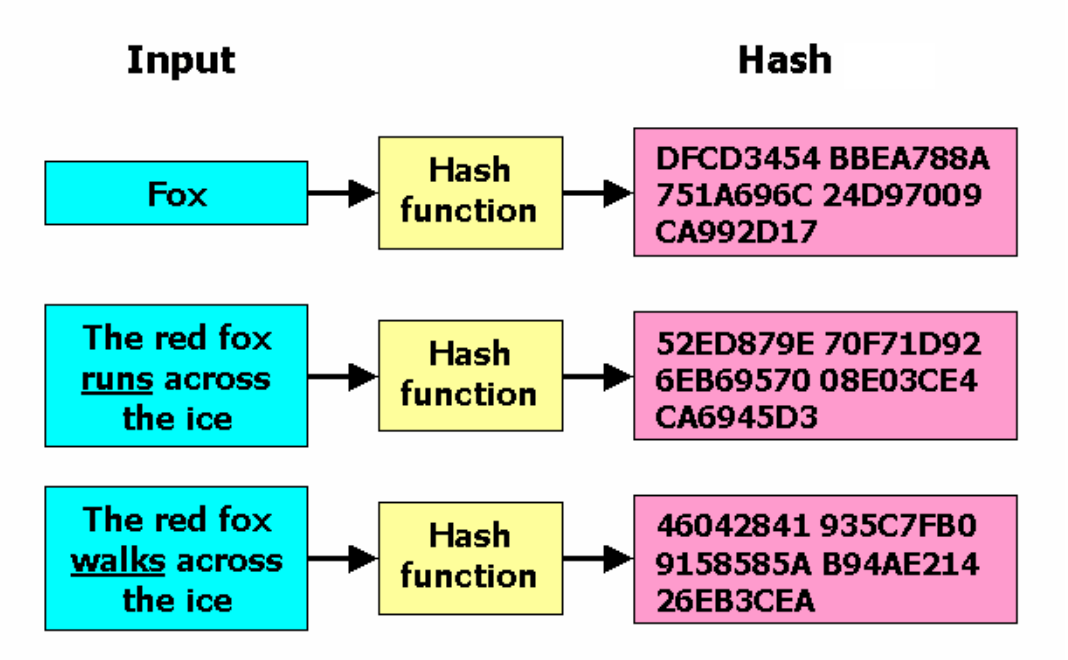
Hashing & Hash 함수

- Hashing은 데이터를 고정된 길이의 (16진법) 숫자로 매핑
- 이때 사용되는 함수가 Hash function
- Hash function으로부터 얻은 결과값을 Hash (해시), Hash value(해시 값), Hash Code(해시 코드), Hash Checksum(해시 체크섬) 이라 부름.
- Hash Code가 다르면 데이터는 확실히 다르지만, 역은 성립하지 않음.



Hashing & Hash 함수

- 암호용 Hash Function (Cryptographic Hash Function)
  - ✓ 대표적인 예로 SHA256 함수가 있음.
  - ✓ Hash Code만을 가지고는 입력 데이터를 도저히 알아볼 수 없게 만든 함수
  - ✓ MD5, SHA계열 함수가 있음

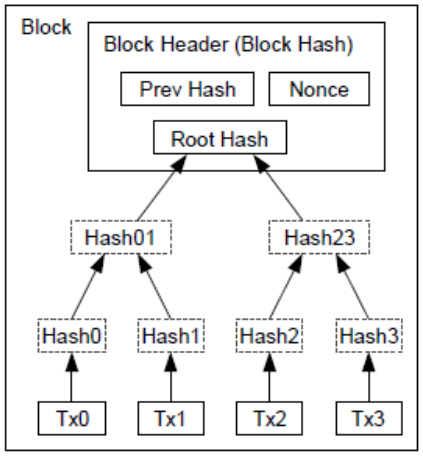


Hashing & Hash 함수

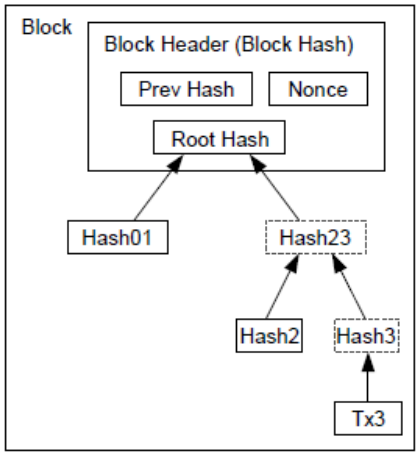
- 한 블록에 존재하는 2800건이 넘는 거래를 Hashing하는 방법
  - ✓ Merkle Tree, Merkle Root 또는 Root Hash 사용

7. Reclaiming Disk Space

Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree [7][2][5], with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.



Transactions Hashed in a Merkle Tree

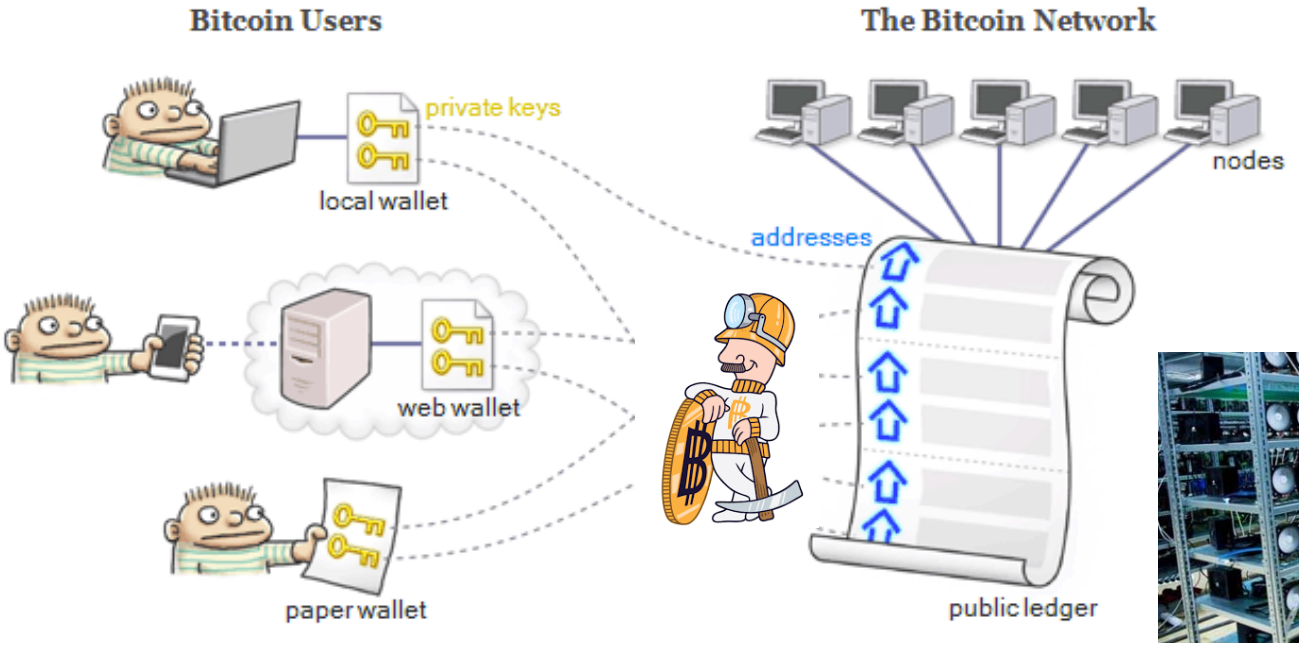


After Pruning Tx0-2 from the Block

(자료원) 사토시 나카모토 논문 4번째 페이지

Node 또는 Miner, 그리고 Bitcoin User

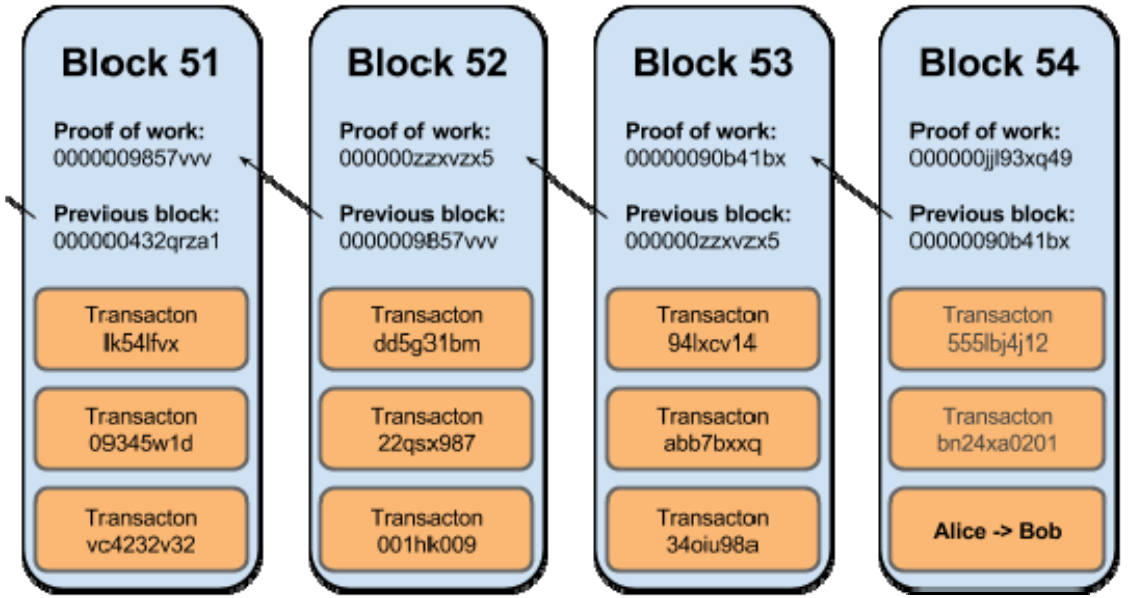
- Node 는 채굴을 통하여 비트코인을 보상 받거나
- 거래를 블록체인에 연결시키는 조건으로 수수료 요구 (대략 $1,25)



블록체인 생성 과정

- 블록체인은 10분 동안에 요청된 거래 기록을 블록체인으로 모아서 암호화시키고,
- Hash Code로 바꾼 후 특정 조건을 만족시키는 “nonce”를 찾아,
- 이를 종합한 최종 Hash Code를 생성하는데 이를 “Proof of work” 라고 한다.
- 블록들은 전의 Proof of work값을 가지고 있음으로써 일관성이 유지됨.

Integrity & Trust를 확보한 분산원장 기술



비잔틴 장군 문제의 해결

- 약 10분 정도 소요되는 채굴과정을 통하여 얻어지는 해쉬코드 구성을 위한 nounce 라는 숫자를 경쟁적으로 찾게 되는데 nounce를 통해 계산된 해쉬코드가 각각의 블록에 체인처럼 연결되어 있다. 따라서 하나의 블록만을 빼내어 위조하려면 전체 블록을 모두 위조해야 하는데 현실적으로 불가능

  현재 블록 수: 489,572개 (2017년 10월 13일, 오전 9시)

- (POW) 채굴을 통해 nounce를 찾는 해쉬코드 경쟁에서 이기면(제일 빠르게 계산하면) 50BTC ➔ 25BTC ➔ 12.5BTC 보상금이 지급되며 이를 통해 총 통화량이 결정됨.

  처음 21만개에서는 50BTC, 21만1 블록부터 42만 번째 블록까지는 25BTC…

  2040년까지 2100만개가 만들어질 예정

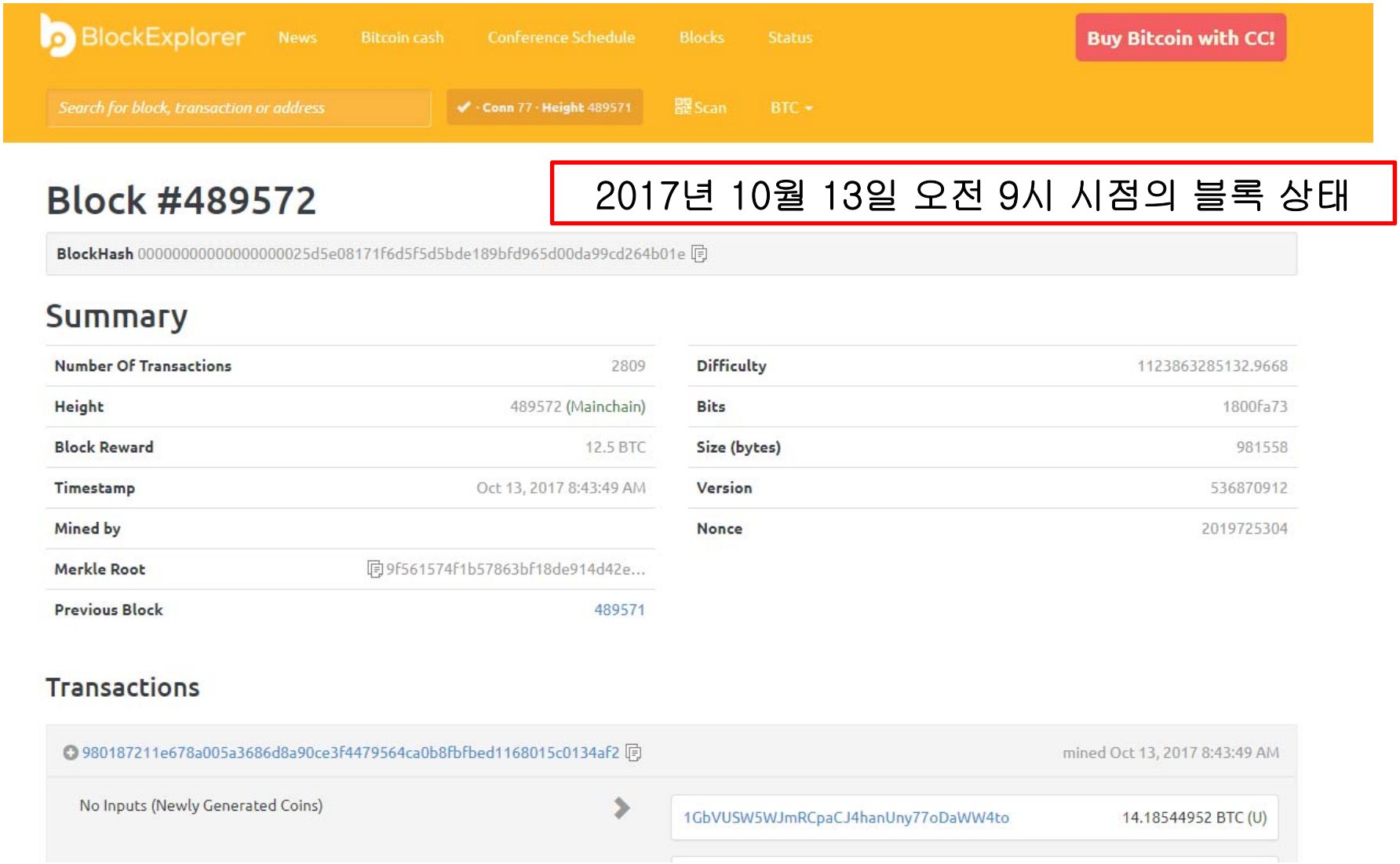
- (합의) Double Spending 문제 방지를 위하여 ‘The longest chain wins’ 적용

  모든 거래내역은 모든 노드에 제공

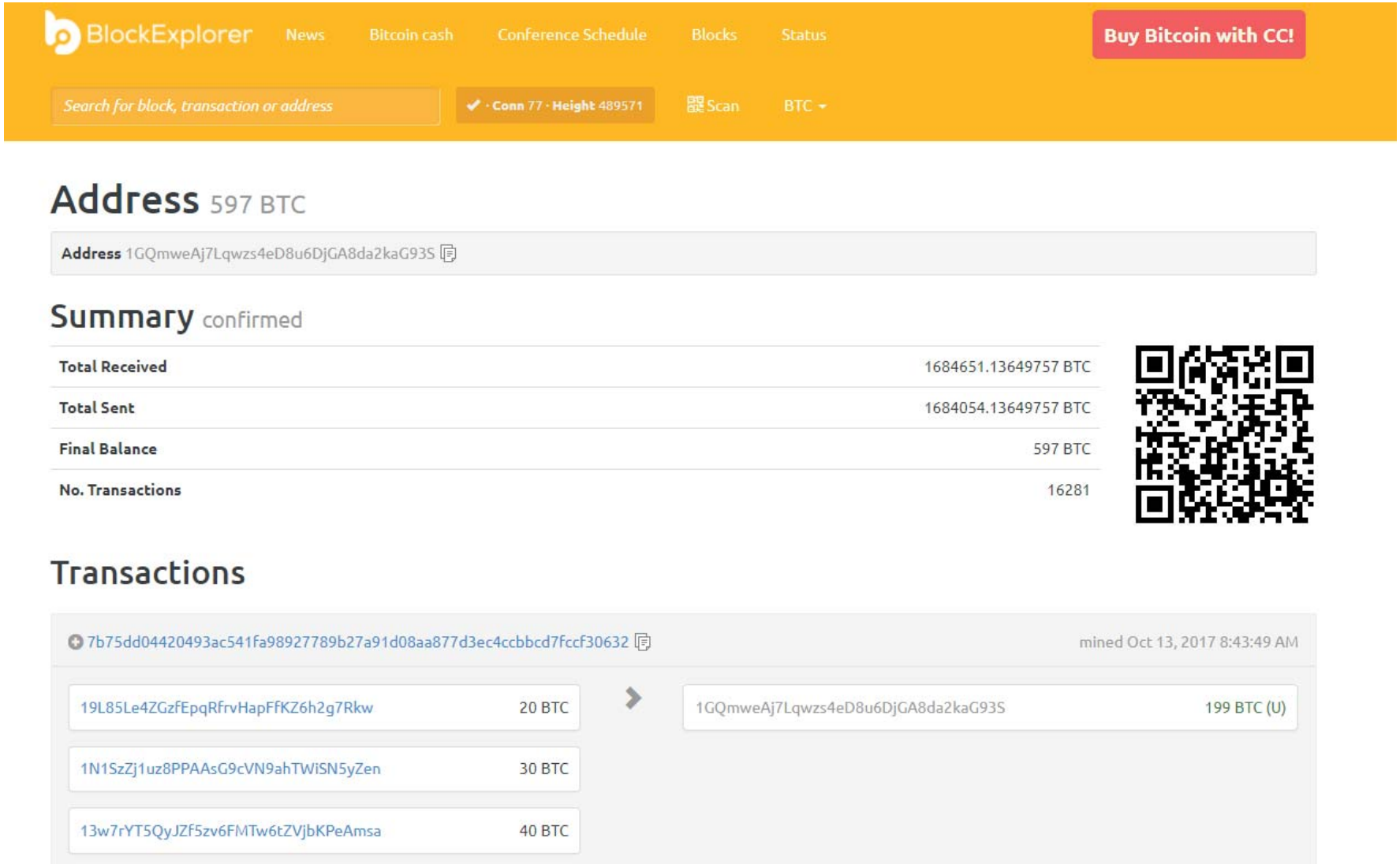
  각 노드에서는 먼저 도달한 거래내역만 저장

  노드들끼리 저장된 정보가 다른 경우는 가장 긴 블록을 공식적으로 채택

블록체인 생성 과정


BlockExplorer
News
Bitcoin cash
Conference Schedule
Blocks
Status
Buy Bitcoin with CC!
Search for block, transaction or address
Conn 77 · Height 489571
Scan
BTC
Block #489572
2017년 10월 13일 오전 9시 시점의 블록 상태
BlockHash 00000000000000000025d5e08171f6d5f5d5bde189bfd965d00da99cd264b01e
Summary
Number Of Transactions 2809
Height 489572 (Mainchain)
Block Reward 12.5 BTC
Timestamp Oct 13, 2017 8:43:49 AM
Mined by
Merkle Root 9f561574f1b57863bf18de914d42e...
Previous Block 489571
Difficulty 1123863285132.9668
Bits 1800fa73
Size (bytes) 981558
Version 536870912
Nonce 2019725304
Transactions
980187211e678a005a3686d8a90ce3f4479564ca0b8fbfbed1168015c0134af2
mined Oct 13, 2017 8:43:49 AM
No Inputs (Newly Generated Coins)
1GbVUSW5WJmRCpaCJ4hanUny77oDaWW4to
14.18544952 BTC (U)

블록체인 생성 과정


BlockExplorer
News
Bitcoin cash
Conference Schedule
Blocks
Status
Buy Bitcoin with CC!
Search for block, transaction or address
Conn 77 · Height 489571
Scan
BTC
Address 597 BTC
Address 1GQmweAj7Lqwzs4eD8u6DjGA8da2kaG93S
Summary confirmed
Total Received 1684651.13649757 BTC
Total Sent 1684054.13649757 BTC
Final Balance 597 BTC
No. Transactions 16281
Transactions
7b75dd04420493ac541fa98927789b27a91d08aa877d3ec4ccbbcd7fccf30632
mined Oct 13, 2017 8:43:49 AM
19L85Le4ZGzfEpqRfrvHapFfKZ6h2g7Rkw 20 BTC
1N1SzZj1uz8PPAAsG9cVN9ahTWiSN5yZen 30 BTC
13w7rYT5QyJZf5zv6FMTw6tZVjbKPeAmsa 40 BTC
1GQmweAj7Lqwzs4eD8u6DjGA8da2kaG93S 199 BTC (U)

블록체인: 비잔틴 장군 문제의 해결 !! ➔ 의미?

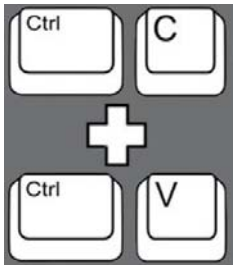
- (인터넷 혁명) 인터넷 등장으로 정보 전달이 원활해짐. 'http://www' 프로토콜의 등장

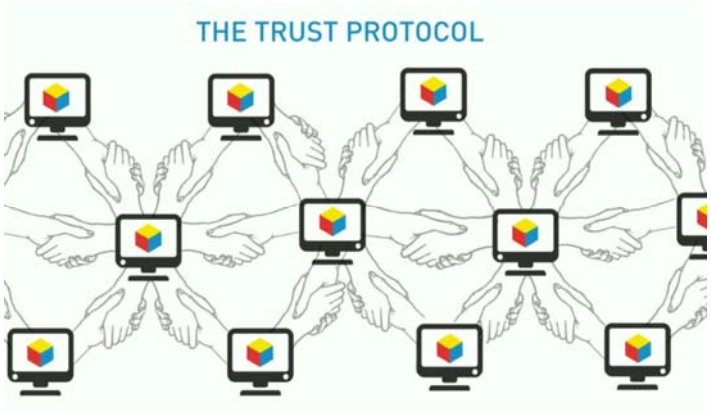
  ➔ (문제점) 'Ctl-C'에 의하여 완벽한 복제가 가능.

  화폐 거래 측면에서는 완벽한 복제는 치명적 결함. (Double Spending Problem)

- (제2의 인터넷 혁명) 인터넷을 통한 가치 전달이 가능해 짐. '블록체인' 프로토콜의 등장

  ➔ 제3자가 개입하지 않고 정보의 진위 여부를 구분할 수 있음.





블록체인의 특징

1. 제3자 개입 없이 P2P 네트워크로 자동으로 작동
2. 거래 내역을 기록한 장부가 분산되어 기록, 보관
3. 장부의 업데이트 및 기록 (블록의 생성)이 사전에 설정한 작업증명(POW: Proof Of Work, 비트코인의 경우는 nonce값) 메커니즘을 통하여 검증되고 승인된다.
4. 암호화(Cryptographic) 기법이 적용되어 보안 유지

- ✓ SHA (Secure Hash Algorithm) 256: 1993년 미국 NSA에서 설계

```
> digest("This is test.", algo="sha256", serialize=FALSE)
[1] "465f0965 7f95d9fe 4d66dda0 f8abf6f2 a7e4ede8 2fb91fdc a9f46bcc 6637cc15“
```

- ✓ ECDSA (Elliptic Curve Digital Signature Algorithm) 암호화 알고리즘: Public Key와 Private Key를 통하여 검증

블록체인이 활용될 수 있는 자본시장 영역

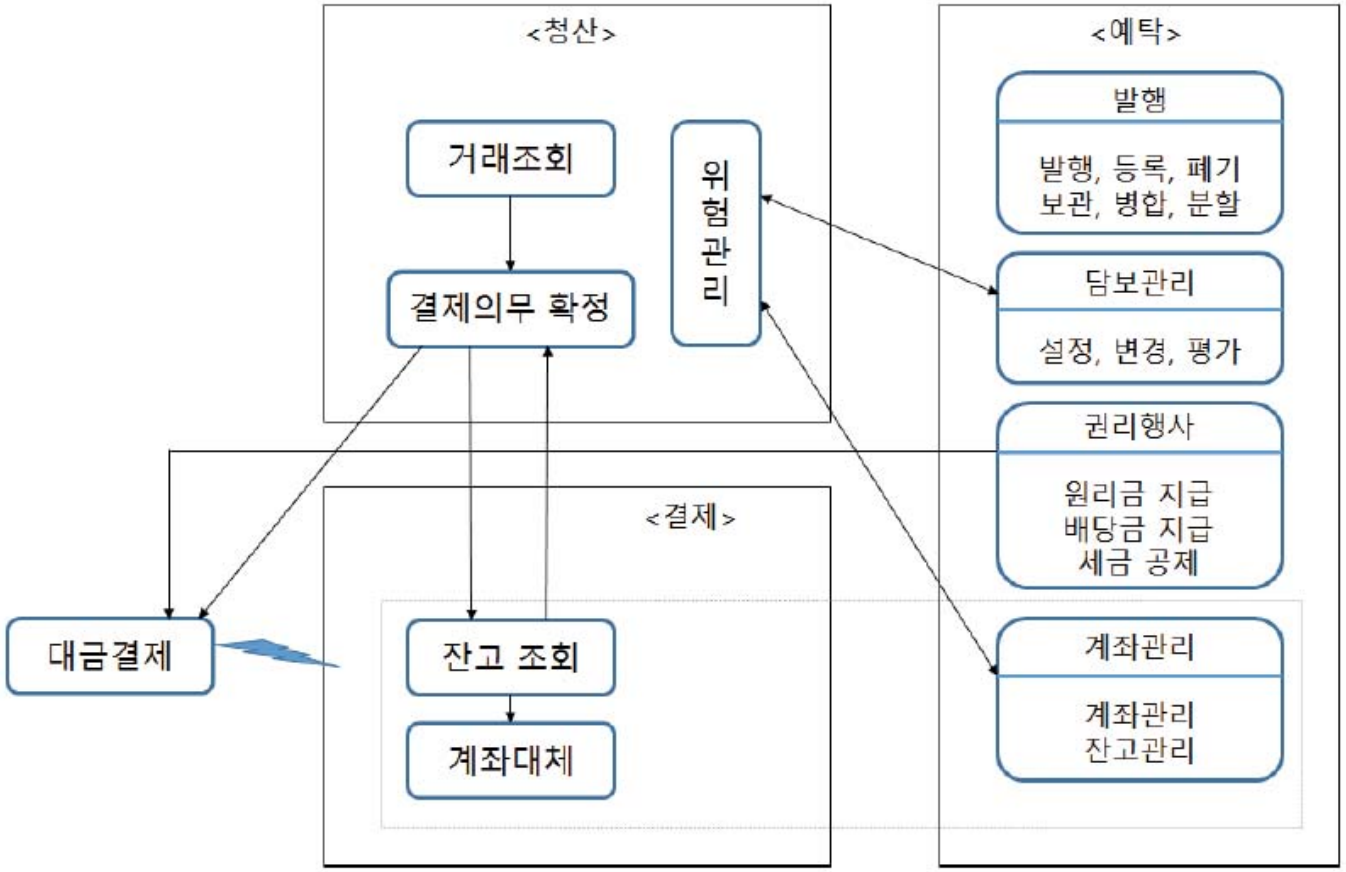
- 가치를 가진 자산의 거래, 소유권 이전, 기록 및 보관이 지속적으로 발생하는 자본시장 영역에서의 블록체인 활용은 매우 유용하게 적용 가능.

- 증권의 발행, 유통 및 거래가 디지털금융 환경이 발전함에 따라
  - ➔ P2P 네트워크 환경 기반 암호화 증권crypto-security 형태로 활성화
  - ➔ 거래소, 청산소, 중앙예탁기관 기능의 축소 및 재정립

- 미국의 NASDAQ, 호주의 ASX에서 실제로 활용되고 있음.
  - 하지만 일반적 발행, 유통 단계 보다는 비공개 기업의 주식 발행 및 거래 그리고 거래 후 처리과정에 활용이 많이 되고 있는 실정

블록체인이 활용될 수 있는 자본시장 영역

거래 후 처리과정 프로세스



자료: 한국예탁결제원(2014)

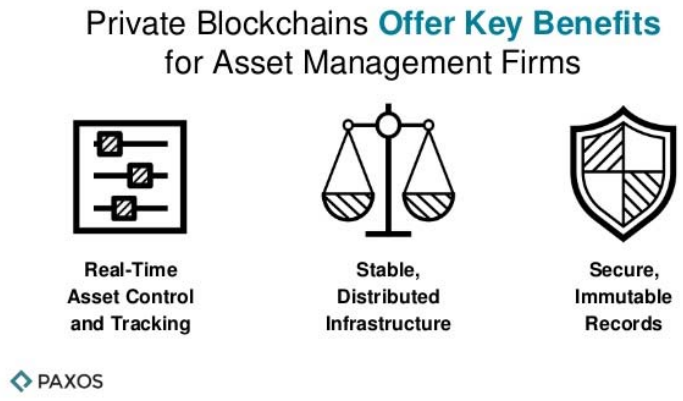
블록체인이 활용될 수 있는 자본시장 영역

- 지급결제 시스템: 금융 인프라 투자 및 유지비용 절감 가능
- 증권의 발행, 거래, 결제: 스마트계약, 동시결제 체계에 적용
  - ➢ 발행: 블록체인 기술을 이용하여 분산장부에 기록됨과 동시에 투자간 거래에 대해서 스마트계약 처리 가능
  - ➢ 거래: 매도자와 매수자 사이에 matching을 통해 매매확인이 이루어지고 private key와 public key를 통해 소유권이 이전되면서 결제가 이루어지며, 분산장부를 통해 기록 및 보관, 이 경우 기존 은행계좌를 연계시키거나 암호화폐를 활용할 수 있음.
  - ➢ 결제: 증권의 종류 (주식, 채권), 거래 방식 (장내거래, 장외거래), 결제방식 (동시결제, 분리경제) 등 다양한 종류의 결제시스템을 커버할 수 있으며, 상호 인증을 통한 '결제의 완결성'을 쉽게 구현할 수 있음.

블록체인의 금융권 적용은 아직은 개발 및 시험, POC 단계
네트워크의 설계? 지배구조? 기술표준?

블록체인이 활용될 수 있는 자본시장 영역

- 자산관리 서비스: 블록체인 기술을 적용하면 펀드매니저의 투자현황을 안전하고 쉽게 파악할 수 있으며, 펀드장부에서 투자자 지분을 간단하게 관리할 수 있음.
  - ➢ 현재는 펀드를 관리하는 경우 증권사, 매도측 은행, 지역 보관기관, 중앙 보관기관, 중앙 예탁기관들이 각각 별도의 계좌를 가지고 관리
- 파생상품: 스마트계약을 통하여 두 당사자 간에 채무를 확정 짓고 청산기관(CCP)에 있는 자산장부에 보관된 자산을 담보장부에 이전하면서 예를 들어, 에스크로 서비스 방식으로 거래 상대방의 신용리스크를 줄일 수 있음.



글로벌 금융권에서의 블록체인 활용 현황

- 2015년 10월 20일 NASDAQ은 블록체인 기술을 시범적으로 도입하여 전문투자자용 장외시장인 Nasdaq Private Market 거래에 활용하는 NASDAQ Linq 플랫폼 발표.
  - ➢ 블록체인 기술을 적용한 결과 주문-결산-승인-펀드 이체 및 디지털 서명-체결-정산이 동시에 이루어지면서 전체 거래 프로세스에 소요 시간을 10분으로 단축
  - ➢ 1초당 수백만 건의 거래를 처리해야 하는 증권거래소의 시스템 요구를 충족시킬 수 있는지는 의문 (비트코인은 1초당 최대 7건, 평균 4.7건)
- 2016년 2월 NASDAQ은 에스토니아 정부와 함께 주주 의결권 행사를 위한 전자투표 서비스 시험운영
- 2016년 5월 Nasdaq Financial Framework 계획 발표 (100개 이상의 관련시장운영기관에 대하여 전 과정의 모든 앱을 통합 관리)
- 특징: 거래빈도가 낮은 매매거래 체결에 활용, 거래참가자를 제한하는 비공개기업의 주식 대상, 예탁-결제-청산과 같은 back office 기능에 활발하게 적용

  호주증권거래소(ASX), 일본거래소그룹(JPX), 영국거래소(LSE) 등이 개발 참여

글로벌 금융권에서의 블록체인 활용 현황

- R3CEV 컨소시엄: 뱅크오브어메리카, 씨티그룹, 골드만삭스, 모건 스탠리, 도이치뱅크, HSBC, UBS를 포함한 50개가 넘는 글로벌 대형 은행들이 참여하여 2015년 9월 미국 블록체인 선두업체인 R3와 제휴해 'R3CEV' (Crypto, Exchanges and Venture practice) 컨소시엄 구성

  - 회원사끼리 블록체인 정보를 공유하고 활용하면서 송금, 결제 등 금융 업무에 적용할 기술개발이나 조사활동을 지원하는 협의체
  - R3는 시스템 설계 및 기술개발 담당
  - 회원사는 자사 API(응용 프로그램 프로그래밍 인터페이스)에 연결해 테스트
  - 블록체인 기반의 해외송금시스템을 우선적으로 개발하여 수수료를 1/10 수준으로 낮출 예정

글로벌 금융권에서의 블록체인 활용 현황

- R3CEV 컨소시엄 (계속)
  - ➢ 국제적인 협력체인 컨소시엄 기반 오픈 소스모델이 세계적인 추세이며, 이에 대표되는 협의체
  - ➢ 적용 분야: 전자어음 발행, 은행 증명서 발급 등과 같은 문서인증, FIDO기반 사용자 인증, 비정상 거래를 적발하는 이상금융거래 탐지시스템(FDS) 등에 활용 타당성을 연구해야 함.
  - ➢ 2016년 4월 POC 영역 발표:

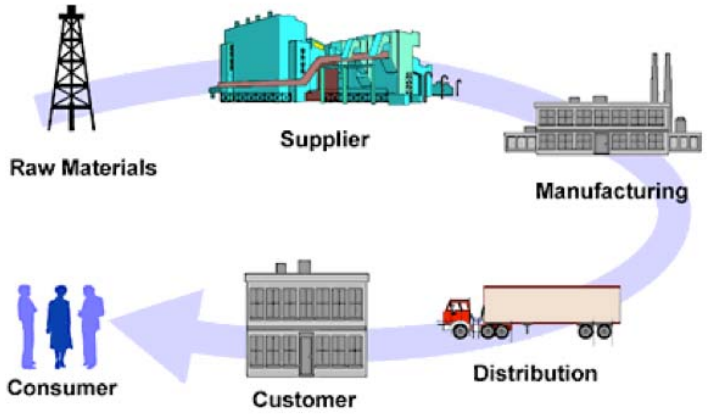
    시스템 연동성, 지급, 결제, 무역금융, 회사채, repo, 스왑, 보험

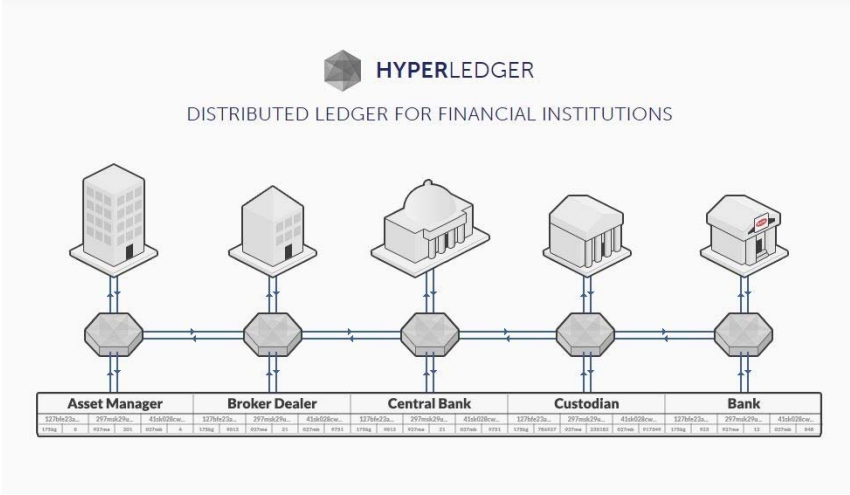
글로벌 금융권에서의 블록체인 활용 현황

- 2016년 1월 11개 은행이 참여 Ethereum 네트워크를 통하여 암호화화폐인 ether를 은행 간 이전하여 정산하는데 성공
- 2016년 4월 금융회산 간 계약의 기록, 관리 및 동기화에 특화된 Corda 플랫폼 발표
  1. 제한된 참여자만 원장을 공유한다.
  2. 중앙 통제기관 없이 금융회사 간 직접 거래가 이루어진다.
  3. 유효성 검증은 개별 거래 차원에서 이루어진다.
  4. 규제 및 감독기관의 참여가 가능
  5. 다양한 합의 메커니즘을 지원
  6. 자체적인 암호화화폐는 발행하지 않는다.

글로벌 금융권에서의 블록체인 활용 현황

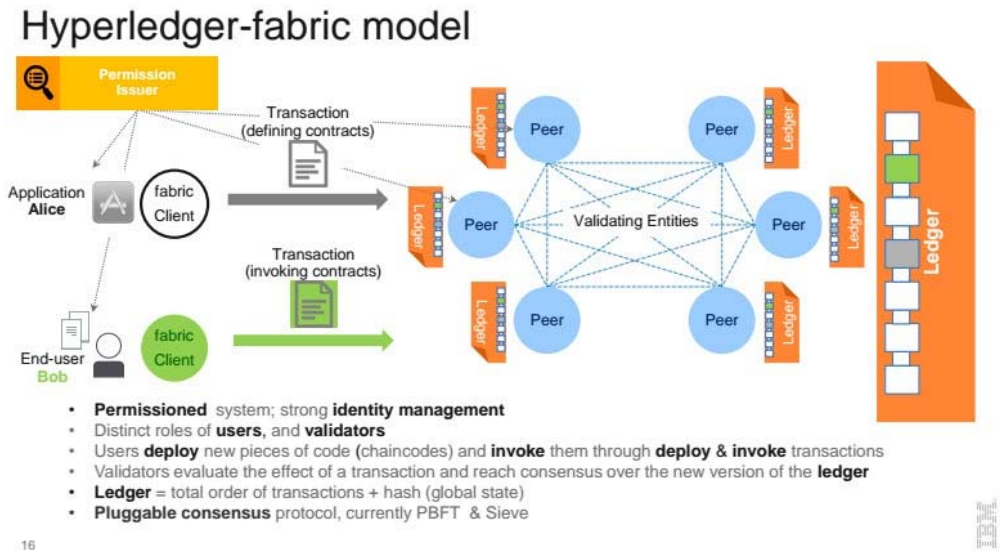
- 리눅스재단이 주도하는 하이퍼레져 프로젝트(Hyperledger Project): IBM, 마이크로소프트, 인텔, 레드햇, VM웨어를 포함한 글로벌 IT회사들이 대거 참여, 국내에서는 한국예탁원과 삼성SDS 참여 ➔ Hyperledger Fabric 소개
  - ➢ 블록체인 기반 무역금융 거래에 대한 분산장부 도입·운영에 대한 테스트 완료
  - ➢ 여기서 정한 프로토콜을 이용하여 은행, 수출업자, 수입업자 간 신용장을 안전하게 발행할 수 있도록 적용하고 있음.
  - ➢ 프리미어 회원은 이사회, 마케팅 위원회 등의 대표를 지정할 수 있음.





글로벌 금융권에서의 블록체인 활용 현황

- 하이퍼레져 프로젝트(HLP) 목표
  - ➢ 산업별 애플리케이션, 플랫폼, 하드웨어 시스템을 구축하고,
  - ➢ 오픈소스 분산원장 플랫폼 개발
  - ➢ Open Source Technical Community 운영
  - ➢ 많은 사용자 및 운영자 확보
  - ➢ 블록체인 활성화를 위한 인프라 기관의 역할 수행



국내 금융권에서의 블록체인 활용 현황

- LG CNS 비상장주식 유통 플랫폼을 개발하였다고 발표
  - 2016년 3월 제정된 '주식,사채 등의 전자등록에 관한 법률' → 시행일은 미정

- 한국거래소는 블록체인 기반 비공개 기업 주식의 장외거래 플랫폼, KPM(KRX Private Market) 사업 추진 계획 발표

- 한국예탁결제원는 Hyperledger 프로젝트에 참여하면서 2017년 9월 섀도보팅 폐지에 따른 블록체인 기반 전자투표 시범서비스 계획을 발표하였으며, 2017년 12월부터는 전자투표 모바일 서비스를 오픈한다고 발표

- 코스콤은 2016년 9월 장외채권 거래시스템의 개념증명이 완료되었고, 2017년 9월에 Hyperledger Fabric 1.0 기반 펀드거래 시스템 개념증명이 완료되었다고 발표

블록체인 관련 사건

- 2014년 2월 비트코인 거래소 중에 가장 규모가 큰 일본에 있는 마운틴 곡스(Mt. Gox)의 파산
  - ➢ 고객 소유의 75만 비트코인과 마운틴 곡스 자사 소유의 10만 비트코인, 도합 85만 비트코인 증발
  - ➢ 일본과 미국을 중심으로 많은 소송이 진행 중
  - ➢ 미국 연방준비제도이사회의 의장은 '제도권에서 비트코인을 규제할 권한이 없다'라고 선언하면서 피해자들에게 어떠한 종류의 보상도 없을 것이라고 설명
  - ➢ 하지만 이 문제는 비트코인 자체의 문제가 아닌 비트코인 거래소의 문제점임을 구분할 필요가 있음. 즉, 화폐의 거래 과정에서 발생한 문제로 이는 블록체인과는 관계없이 디지털 화폐로 소유가 이전되는 과정에서 항상 나타날 수 있는 문제
  - ➢ 또한 제도적인 장치가 미흡하여 투기와 해킹 공략의 대상이 되었다는 측면을 심각하게 생각하여야 하고 이에 대한 제도적 개선 방향을 잡아야 할 것임.

➢ 2016년 DAO 해킹 사건

블록체인에 대한 법제적 환경

- 블록체인에 대하여 관여할 법적인 근거가 없으며, 따라서 이에 대한 금융감독 기준이 존재하지 않음

  - ➢ 분산원장을 이용하는 경우, 누가 누구에게 어떠한 규제를 받아야 하는지에 대한 명확한 역할 분담이 필요
  - ➢ 특별히 규제기관이 블록체인 기술에 참여할 수 있는 법적 개입근거가 필요
  - ➢ 블록체인을 공공적 성격을 가진 금융시장의 인프라로 이용하는 경우, 네트워크 상에 나타나는 실시간 거래의 한계 및 대용량 데이터 처리 한계를 이해하고, 법률적 측면에서의 노드 선정, 감시 및 감독의 필요성 여부, 과세 원칙 등 다양한 문제 해결을 위한 원칙이 수립되어 있어야 함.
  - ➢ 기술표준, 네트워크 지배구조, 참여기관들의 이해 조정, 네트워크 비용 분담 등의 문제를 논의, 합의, 조정할 수 있는 조직이 필요

블록체인에 대한 법제적 환경

- 블록체인 관련 법적인 분쟁이 발생 시 해결을 위한 접근 원칙이 부재
  - ➢ 빅브라더 문제를 포함하여 법적 분쟁이나 소송이 진행되는 경우 사법적 처리를 위한 규제기관 개입에 대한 적법성과 증거 수집을 위한 원칙과 절차 필요

- 블록체인의 분산성으로 금융실명제와 익명성 추구에 상충 문제가 대두될 수 있음.

- 블록체인 활성화를 위해서는 현재 금융IT 감독체계는 중앙집중식, 폐쇄성에서 크라우드 기반 분산형, 개방식으로 전환하는 규제완화 정책이 요구
  - ➢ 현재의 금융기관 시스템은 처리속도, 해킹방지, 위변조방지, 불법적 거래, 조세회피를 방지하기 위하여 전용선, 폐쇄망을 기반으로 하는 중앙관리 시스템을 의무화하고 있으므로 이에 대한 인식 전환이 필요하며, 이에 대한 법적 근거도 함께 필요

End of Document