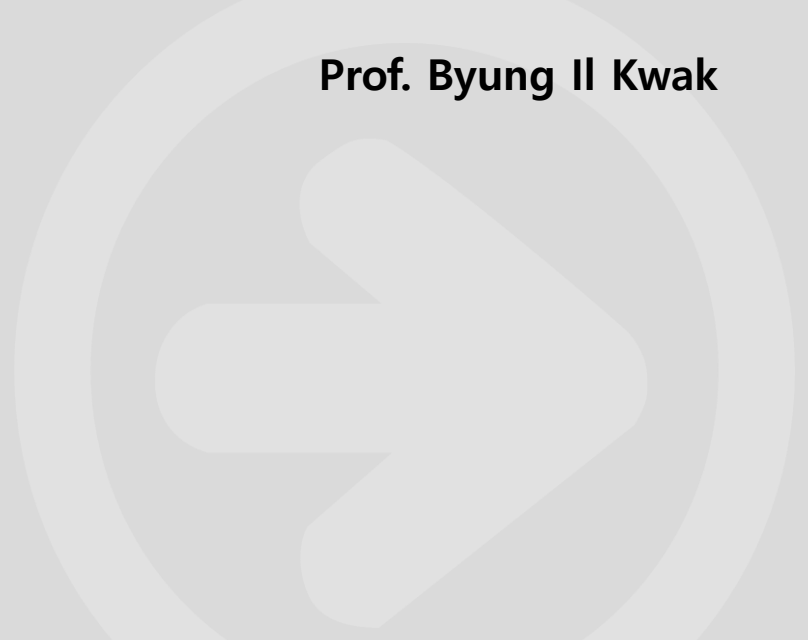




Blockchain #2

The basic features of blockchain

Prof. Byung Il Kwak



CONTENTS

- ❑ 블록체인 소개
 - ❑ 블록체인의 정의
 - ❑ 블록체인의 역사
 - ❑ 블록체인의 기본 특징

Introduction of blockchain

□ 블록체인 (Blockchain) 정의

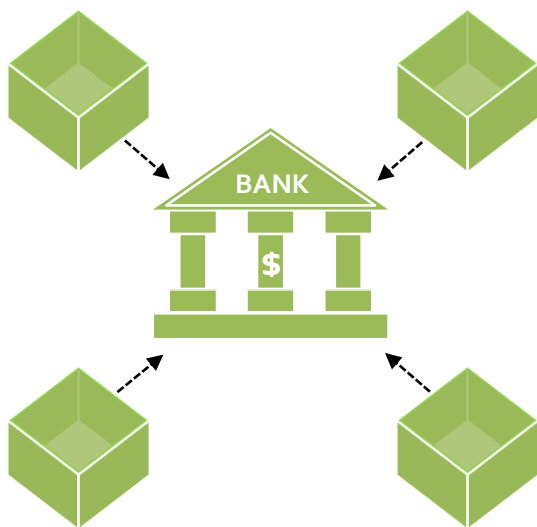
- ▣ P2P (Peer to Peer) 네트워크를 이용한 분산 데이터베이스 기반의 저장 기술
 - 분산원장 기술 (DLT: Distributed Ledger Technology)로도 불리며, 거래 정보 (Transactions)를 기록한 원장 데이터를 블록체인에 참여한 여러 노드들이 공동으로 기록 및 관리하는 것
- ▣ 즉, **블록체인 네트워크에 연결된 여러 컴퓨터에 거래 정보가 담긴 원장 데이터를 저장 및 보관하는 기술**

Introduction of blockchain

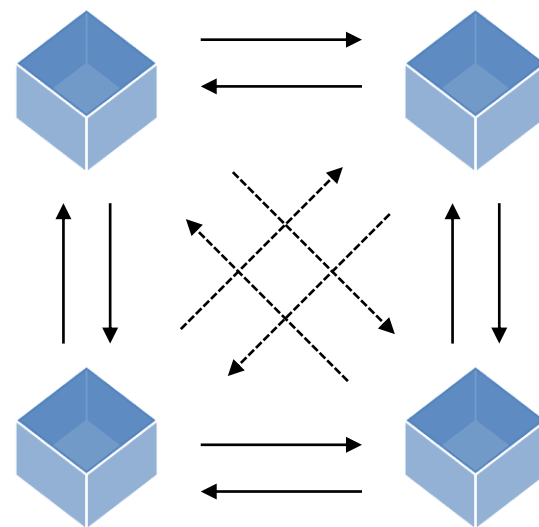
❑ 블록체인

❑ 분산 공개 장부

- 블록체인에 연결된 모든 사용자들은 동일한 장부 (데이터)를 공유하고 저장함으로써, 기존 거래 방식에서의 중앙 관리가 없이 투명 (Transparency) 하게 내역을 관리함



기존 거래 방식



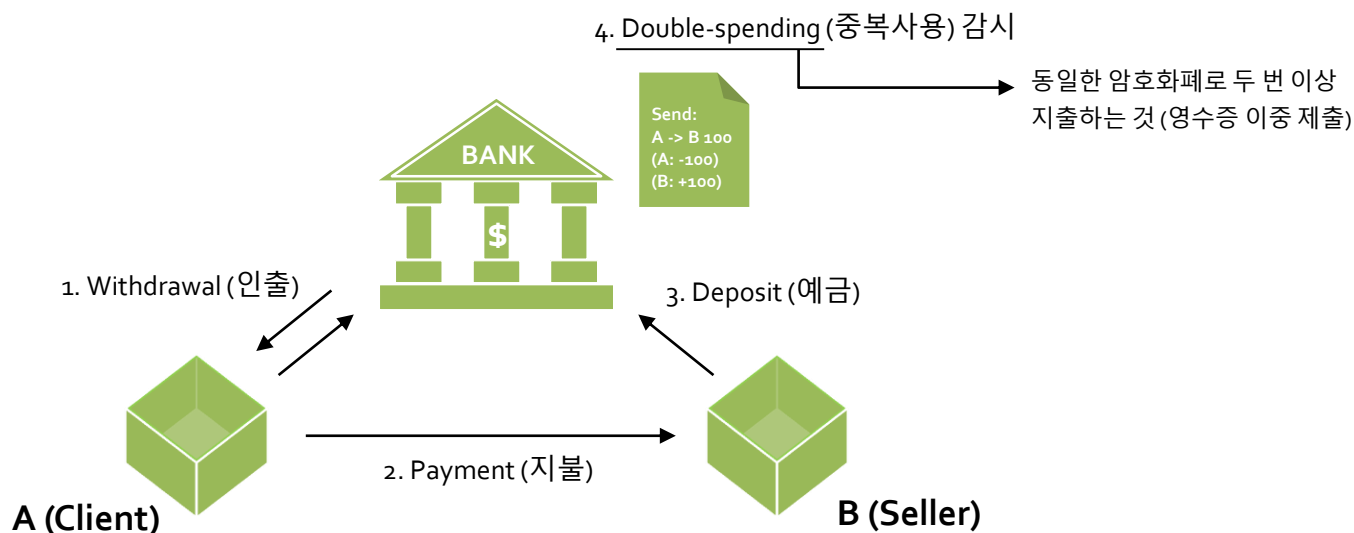
블록체인 거래 방식

Introduction of blockchain

블록체인

기존 거래 방식

- 중앙 은행이 모든 거래 내역을 가지고 있음
- A가 B에게 100원 송금한 사실을 중앙은행이 증명함
- 거래 당사자들은 신뢰할 수 있는 중앙은행에게 거래내용에 대한 증명을 모두 맡기는 형태

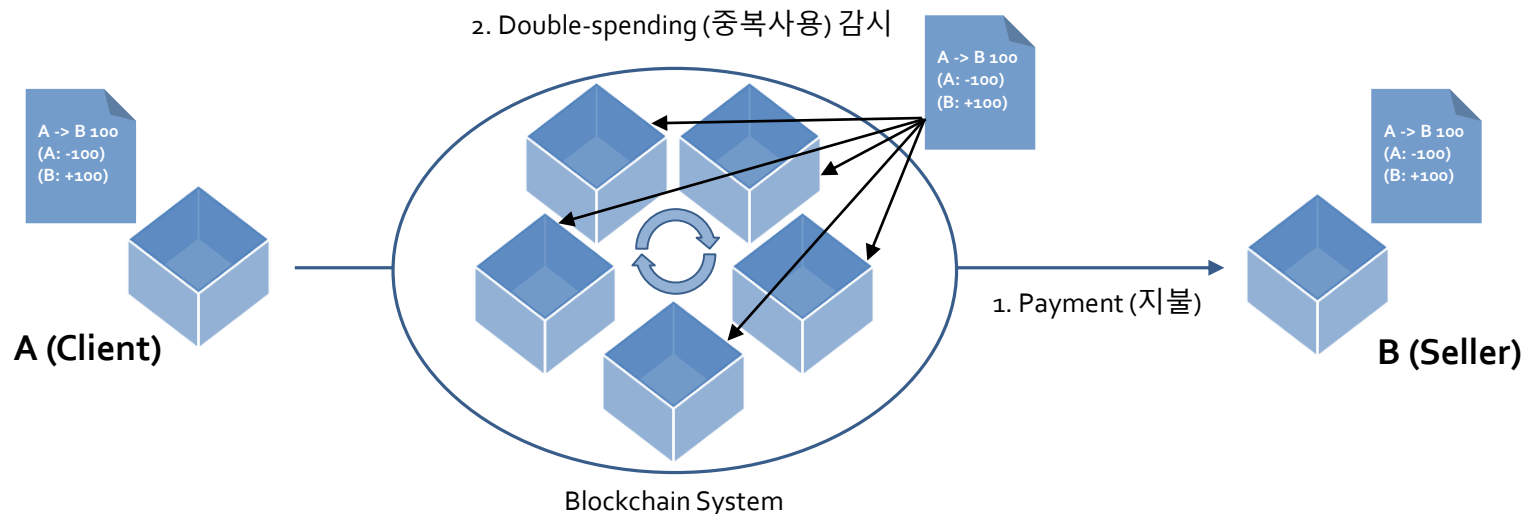


Introduction of blockchain

□ 블록체인

▣ 블록체인 거래 방식

- 거래 내역을 중앙은행이 아닌 여러 곳에 저장함 (분산형태)
- A가 B에게 100원 송금한 사실을 참여하고 있는 모든 노드들에게 저장함
- 블록체인에 참여한 모든 노드들이 송금(거래)한 사실을 증명함





Introduction of blockchain

블록체인

현금, 디지털화폐, 가상화폐와 암호화폐 비교

현금, 디지털화폐, 가상화폐와 암호화폐 비교

	현금(법정통화) Fiat Currency	디지털 화폐 Digital Currency	가상화폐 Virtual Currency	암호화폐 Cryptocurrency
				
화폐 형태	주화(금속) 또는 지폐(종이)	디지털	디지털	디지털
화폐 구분	법정통화	법정통화	가상화폐	암호화폐
적용 법규	○	○	X	X
사용처	모든 거래	가맹점	가상공간	가맹점
발행기관	중앙은행	금융기관	비금융기관	X
법정통화와의 교환성		법정통화로 충전, 잔액은 법정통화로 환급가능	가상화폐를 법정통화로 교환할 수 없음	법정통화와 자유로이 교환됨

자료: 한국은행, 피넥터, 유진투자증권

Introduction of blockchain

□ 블록체인의 역사

■ 1983. Blind Signature (은닉서명) 기술 개발 (David Chaum)

- Untraceable Electronic Cash (추적 불가능한 DigiCash 개발)
- 거래 당사자의 신분을 노출시키지 않고 결제 사실을 검증하는 기술
- 해당 기술에서 제안한 디지털 서명과 암호학 관련 개념들이 암호화폐의 기본 원리를 가지고 있음

■ 1989. DigiCash 설립 (David Chaum)

- 암호화, 개인키 및 공개키, 블라인드 서명 기술 적용한 전자 결재를 통해 Ecash 디지털 화폐 운영 시작
- However, 보편화되고 더 편리한 신용카드로 인해 실패
 - 이때 당시, 편리성 >>> 프라이버시 보호

Introduction of blockchain

□ 블록체인의 역사

▣ 1997. HashCash 기술 개발 (Adam Back)

- 대량의 Email Spam과 DoS 공격을 막기 위한 PoW (Proof of Work) 시스템으로 HashCash 제안
 - Email 발송시, HashCash 스탬프를 받아야만 발송 가능
 - HashCash 스탬프를 받기 위해서는 컴퓨터 연산을 통해 일정 Hash 값을 찾도록 하는 PoW (작업증명) 과정이 필수

▣ 1998. Bit Gold 기술 개발 (Nick Szabo)

- 가상화폐의 원리와 구조를 고안 (비트코인의 기원)
- 탈중앙화 디지털 화폐로 참여자들이 컴퓨팅 자원을 통해 암호화 퍼즐을 푸는 방식
- 같은 네트워크에 있는 다수가 유효한 판정을 내려야 다음 퍼즐로 옮겨갈 수 있음
- 디지털 화폐의 이중지불 문제 해결에 기여

Introduction of blockchain

□ 블록체인의 역사

▣ 1998. B-Money 제시 (Wei Dai)

- 각 참여자들의 B-Money 보유 정보를 모든 참여자들이 별도의 데이터베이스에 해시함수로 저장하여 서로 간의 연결된 블록으로 저장
- 새로운 블록을 추가 시, 가장 먼저 암호를 풀은 참여자에게 B-Money 인센티브를 주는 작업증명(PoW)과 보유한 암호화폐의 양에 기반하여 일부 참여자에게만 인센티브를 주는 지분증명(Proof of Stake) 방법 제안

Introduction of blockchain

□ 블록체인의 역사

▣ 2008. Bitcoin

- 2008년 사토시 나카모토의 "Bitcoin: A Peer-to-Peer Electronic Cash System" 공개
- 2009. 사토시 나카모토 (가명)라는 사람이 C++ 언어를 기반으로 Bitcoin 개발
- 2009.1.3 최초의 Bitcoin 블록인 제네시스 블록 (genesis block)을 생성

Introduction of blockchain

□ 블록체인의 역사

▣ Bitcoin

Bitcoin: A Peer-to-Peer Electronic Cash System

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

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

탈중앙화 개념

블록들의 체인 형태

Introduction of blockchain

□ 블록체인 활용

- ▣ 비트코인 (거래 및 송금 액수)
- ▣ 자산 기록 (소유 동산 및 부동산 정보)
- ▣ 물류 유통 (화물 유통 정보)
- ▣ 스마트 컨트랙트 (도박, 중개거래, 이커머스, 물품 거래)
- ▣ 전자 투표
- ▣ 의료 보험



Introduction of blockchain

❑ 블록체인 활용

Blockchain industry applications



Automotive (222 KB)



Banking and financial services



Government



Healthcare and life sciences



Insurance



Media and entertainment



Retail and consumer goods



Telecommunications



Travel and transportation (340 KB)



Supply chain



Oil and gas



Manufacturing



<https://www.ibm.com/blockchain/industries>

Introduction of blockchain

- 블록체인의 기본 특징
 - ▣ 분산 원장 (Distributed ledger)
 - ▣ 암호화 (Cryptography)
 - ▣ 합의 (Consensus)
 - ▣ 스마트 컨트랙트 (Smart Contract)

Introduction of blockchain

❑ 블록체인의 기본 특징

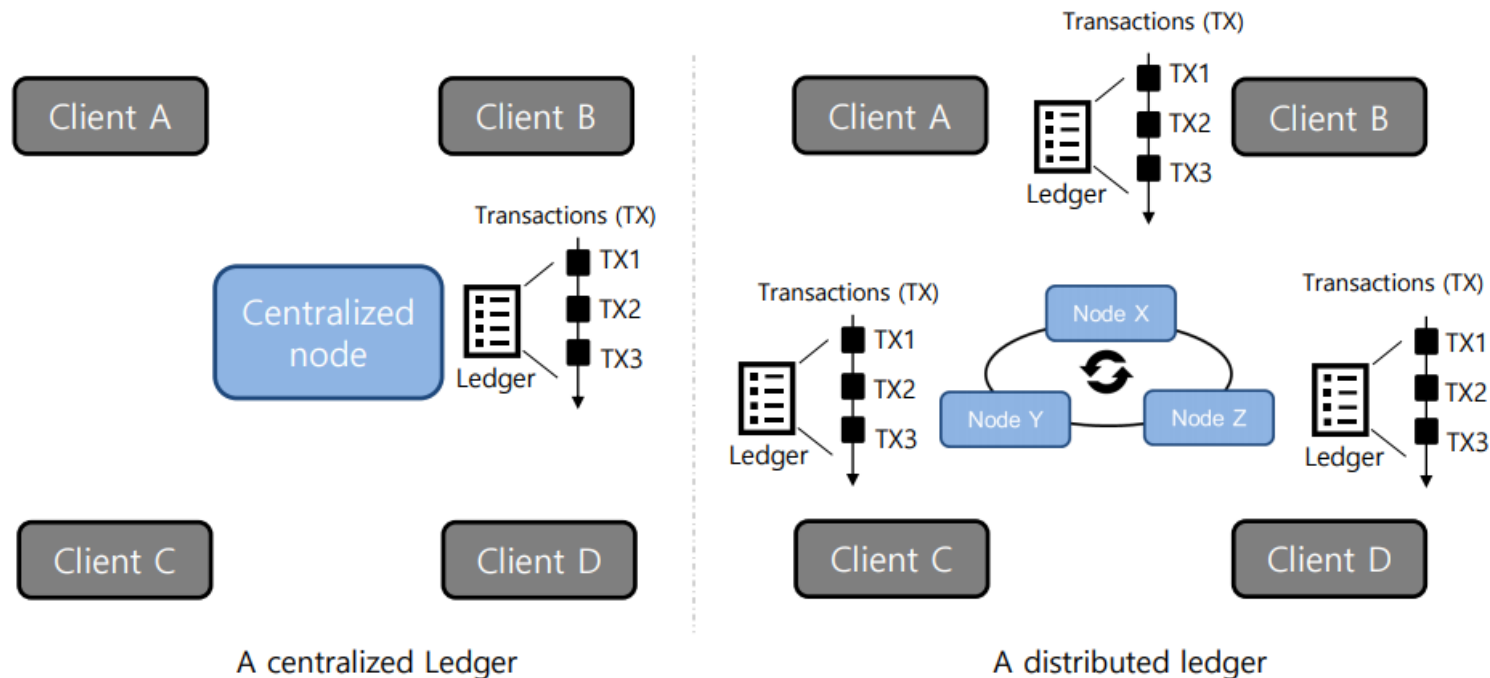
▣ 분산 원장 (Distributed ledger)

- History of all transactions
 - 과거의 거래기록부터 현재까지의 거래 기록들이 블록들로 저장 및 연결되어 있음
- Append-only with immutable past
 - 블록들이 체인으로 연결되어 있어, 중간의 블록이 변경되면, 기존의 형태대로 블록을 연결하여 저장할 수 없음
- Distributed and replicated
 - 블록체인에 저장된 데이터는 P2P 방식으로 블록체인 네트워크를 구성하는 모든 노드들에 복사되어 동일한 자료를 저장함



Introduction of blockchain

- 블록체인의 기본 특징
 - 분산 원장 (Distributed ledger)



Blockchain adopts a distributed way

Introduction of blockchain

❑ 블록체인의 기본 특징

❑ 암호화 (Cryptography)

– Integrity of transactions

- 거래기록 장부는 네트워크의 참여 노드들 모두가 공동으로 소유하여, 거래 데이터 조작을 방지하고 해시(Hash) 값을 통해 무결성 보장

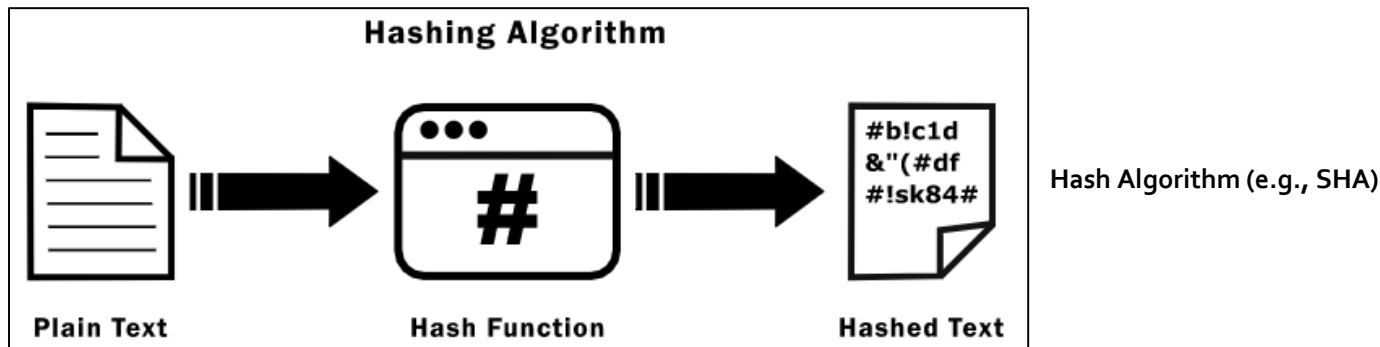
– Authenticity of transactions

- 각 거래 (transaction)에 있어서, 전자 서명 알고리즘을 통해 거래의 정당성을 보증
 - “Transaction: A -> B, 10 BTC”은 비대칭키 암호화 방식 (Public key and private key) 이용한 전자 서명
 - 이를 통해, 아래 사항들을 확인할 수 있음
 - 제3자의 트랜잭션 내용 위변조
 - 제3자의 도용을 통한 트랜잭션을 수행
 - 코인의 정당한 소유자에 대한 트랜잭션 수행 여부

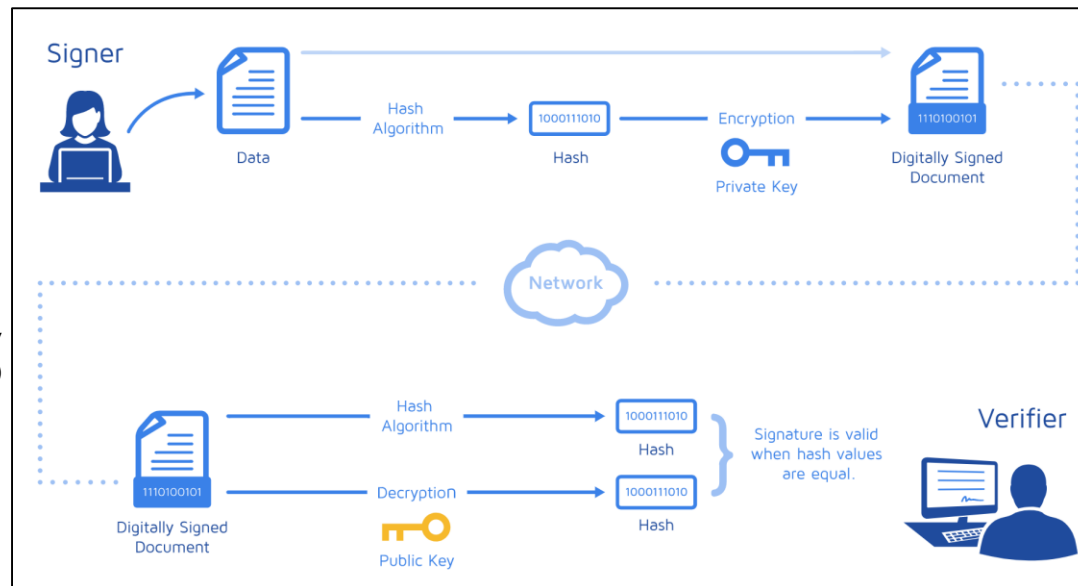
Introduction of blockchain

블록체인의 기본 특징

암호화 (Cryptography)



Digital Signature with Asymmetric cryptography (e.g., ECDSA)



Introduction of blockchain

❑ 블록체인의 기본 특징

❑ 합의 (Consensus)

– Decentralized Protocol

- P2P 네트워크와 같은 분산 네트워크에서의 합의 형성을 수행

– Transactions validated

- 거래를 검증하기 위해, 블록체인 네트워크의 각 노드에서 만들 블록의 정당성을 검토

– Data discrepancy managed

- P2P 네트워크에서 정보의 지연 및 수신에 안되는 문제점을 해결하기 위해 합의 알고리즘 사용

Introduction of blockchain

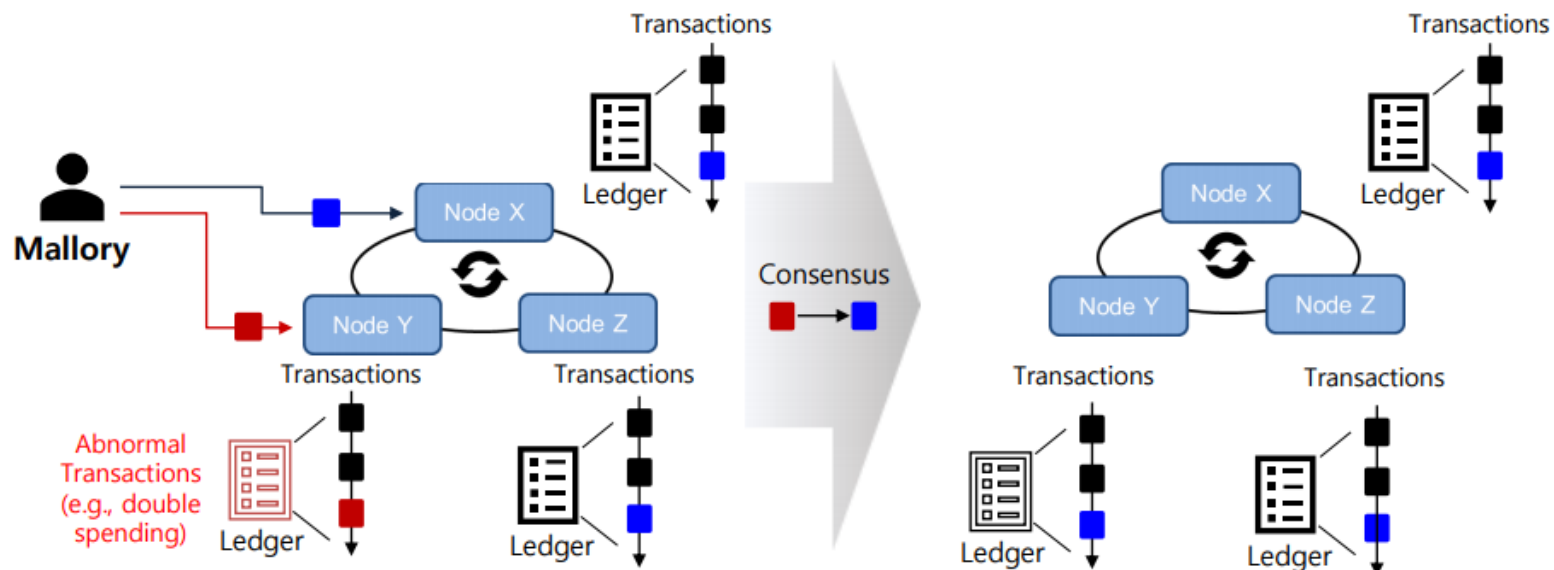
블록체인의 기본 특징

합의 (Consensus)

Mallory has 3 bitcoins, but Mallory can try following two conflict transactions

■: Mallory transfer 3 bitcoins to Alice

■: Mallory transfer 3 bitcoins to Bob



Introduction of blockchain

□ 블록체인의 기본 특징

▣ 스마트 계약 (Smart Contract)

- 넓은 의미의 스마트 계약

- 여러 사람이 합의한 내용(계약)을 사람(신뢰할 만한 중간 담당자 - Trusted Third Party)이 없어도 자동으로 실행

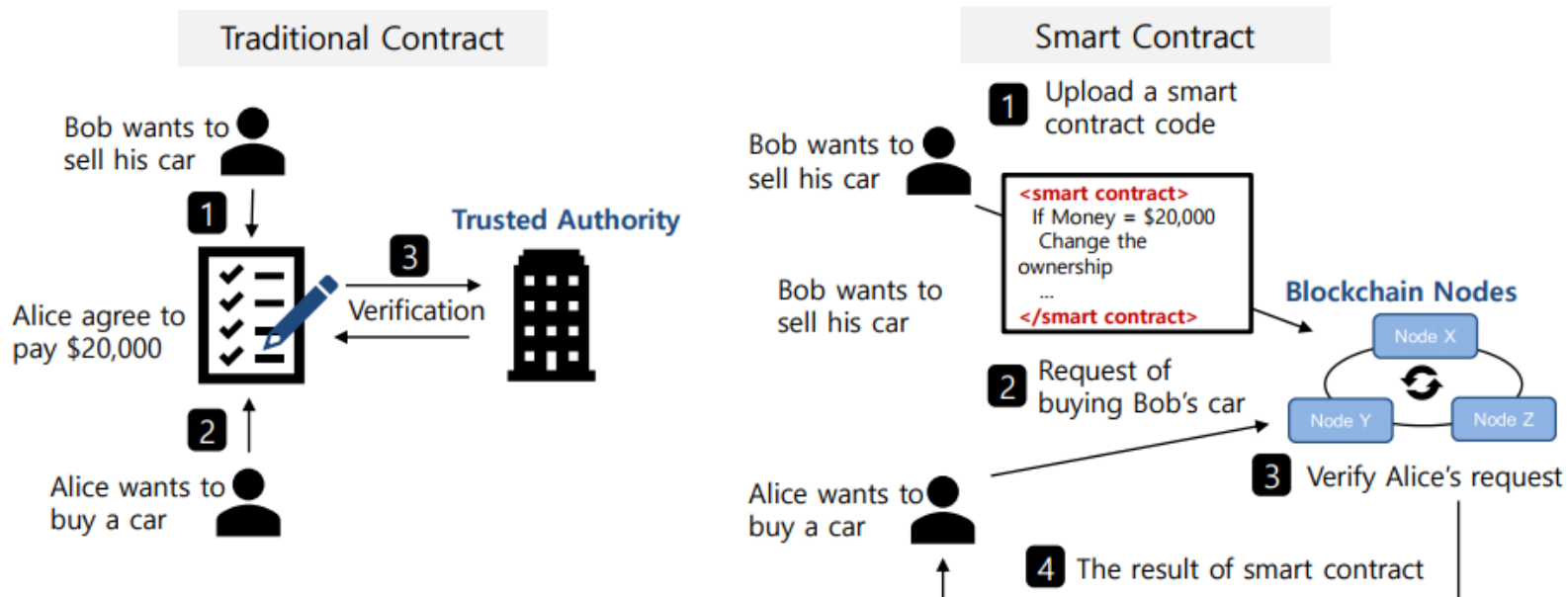
- 블록체인의 스마트 계약

- 다수의 노드가 같은 데이터를 공유하고, 검증하는 방식을 통해 각 노드들은 스마트 계약 내용이 저장된 블록들을 공유됨
- '과거의 기록'이 아닌 '미래에 일어날 일'(계약)을 미리 기록할 수 있으며, 블록체인을 이용하여 해당 계약을 생성후 자동으로 실행

Introduction of blockchain

블록체인의 기본 특징

스마트 계약 (Smart Contract)



CONTENTS

- ▣ 비트코인 소개

- ▣ 암호화폐

- ▣ 신원인증

- ▣ 기록 관리

- ▣ 합의

Introduction of Bitcoin

비트코인 (Bitcoin)

암호화폐 (Cryptocurrency)

- 비트코인은 대표적인 암호화폐 중 한 개
- 2009년도에 개발 및 배포됨
- 현재 6074개의 암호화폐가 CoinMarketCap에 등록됨



CoinMarketCap | 암호화폐 | 거래소 | NFT | 포트폴리오 | 관심 목록 | Calendars | 상품 | 배우기

Want to take a sneak peek of our enhanced homepage? | Yes, switch to new home

시가총액에 의한 최고 100 암호화폐

글로벌 암호화폐 시가 총액은 ₩2234.93T, 마지막날 ▲0.21% 증가했습니다 [더 읽기](#)

☆ 관심 목록 | 포트폴리오 | **암호화폐** | 카테고리 | DeFi | NFT | Play To Earn | Polkadot | BSC | Solana | Heco

#	▲	이름	가격	24h %	7d %	시가총액	거래량 (24시간)
☆ 6071		Baby Doug BABYDOUG	₩0.000342	▲0.75%	▼1.92%
☆ 6072		Staked ICX siCX	₩1,426.07	▲2.18%	▼0.32%
☆ 6073		Balanced Dollars bnUSD	₩1,155.83	▲2.30%	▼0.32%
☆ 6074		Balanced Token BALN	₩2,538.75	▼0.31%	▼0.32%

6001 보이기 - 6074 의 6074

< 1 ... 57 58 59 60 **61** >

Introduction of Bitcoin

□ 비트코인 (Bitcoin)

▣ 암호화폐 (Cryptocurrency)

- 계좌 및 신원 관리 (ID, password, public certificate)
- 화폐 지급 (Transfer, withdraw money)
- 신용 관리 (Account history)
- 신뢰성 (Hash chain)



Bitcoin

Introduction of Bitcoin

□ 비트코인 (Bitcoin)

▣ 신원인증 (Identity)

- 일반적인 통화 (Currency)에서의 신원인증이 필요한 이유
 - 화폐 대차 (saving, loan)
 - 화폐 지급 (transfer)
 - 신용 관리
- 현실에서의 신원 인증
 - 집 주소 및 현관문 키와 비밀번호
 - 이메일 주소 및 비밀번호
 - 계좌 번호, 계좌의 비밀번호
 - 비트코인 공개키(public key), 개인키 (private key)

Introduction of Bitcoin

□ 비트코인 (Bitcoin)

▣ 신원인증 (Identity)

- 비트코인에서의 **공개키**와 **개인키**는 일반 은행에서의 **계좌번호**와 계좌의 **비밀번호**에 해당
- 비트코인의 계좌에서 다른 계좌로 전송할 경우, 해당 계좌 (**공개키**)에 대한 계좌 비밀번호인 **개인키**가 필요

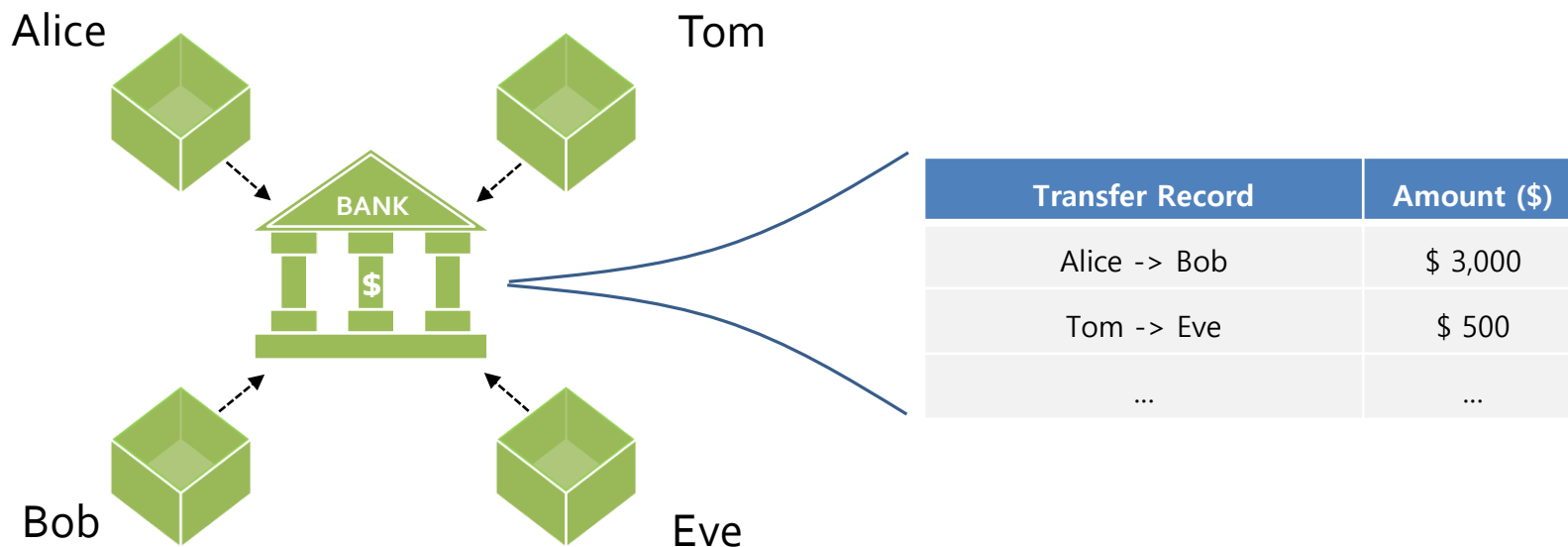


Introduction of Bitcoin

□ 비트코인 (Bitcoin)

▣ 기록관리 (Record management)

- Alice가 Bob에게 3000\$ 송금, Tom이 Eve에게 500\$ 송금
 - 중간의 신뢰할 만한 은행에서 위의 거래 관련 정보를 장부에 기록
 - 은행에서의 장부를 통해, 모든 거래들이 추적 가능



Introduction of Bitcoin

□ 비트코인 (Bitcoin)

▣ 기록관리 (Record management)

– Alice가 Bob에게 3 BTC 송금, Tom이 Eve에게 0.5 BTC 송금

■ 블록체인의 연결된 모든 노드들이 **"Alice -> Bob, 3 BTC"**, **"Tom -> Eve, 0.5 BTC"**에 대한 거래 기록을 가지고 있음

■ 특정 계좌만을 이용한 거래들의 추적이 가능

Transfer Record	Amount (BTC)
Alice -> Bob	3 BTC
Tom -> Eve	0.5 BTC
...	...

Alice



Tom



Bob



Eve



Transfer Record	Amount (BTC)
Alice -> Bob	3 BTC
Tom -> Eve	0.5 BTC
...	...

Transfer Record	Amount (BTC)
Alice -> Bob	3 BTC
Tom -> Eve	0.5 BTC
...	...

Transfer Record	Amount (BTC)
Alice -> Bob	3 BTC
Tom -> Eve	0.5 BTC
...	...

Introduction of Bitcoin

□ 비트코인 (Bitcoin)

▣ 합의 (Consensus)

- 비트코인은 블록체인의 분산형 원장을 활용한 거래 이력 공유 및 검증을 수행
- But, 이중지불 문제 (Double spending attack)의 가능성 존재
- Longest chain 합의를 악용한 거래 내용을 변조하고 부당이득을 취하는 공격
 - 쉽게 말하면, 총 자산 10 BTC를 가지고 있는 **Alice**가 **Bob**에게 5 BTC를 전송하는 거래와 Alice가 Tom에게 5BTC를 전송하는 거래를 동시에 수행하는 공격
- 이중지불 문제를 해결하기 위해 "합의 알고리즘" 필요

Introduction of Bitcoin

□ 비트코인 (Bitcoin)

▣ 합의 (Consensus)

- 다수의 참여자들이 통일된 의사결정을 위해 사용하는 알고리즘 (합의 모델, 합의 방식, 합의 메커니즘, 합의 프로토콜)
 - 블록체인 네트워크에 참여한 모든 노드들이 동일한 거래 기록을 공유하기 위해 사용하는 알고리즘
- 합의 알고리즘의 종류
 - 작업증명 (Proof of Work)
 - 지분증명 (Proof of Stake)
 - 위임지분증명 (Delegated Proof of Stake)
 - 외에도 다양한 합의 알고리즘 존재
- 비트코인에서는 **PoW** 합의 알고리즘을 사용

Introduction of Bitcoin

- 비트코인 (Bitcoin)
 - ▣ 합의 (Consensus)

Proof-of-Work

Evidence

Spent resources



■ 합의 (Consensus)

					3		8	5
		1		2				
			5		7			
		4				1		
	9							
5							7	3
		2		1				
				4				9

Easy problem

[illegible]

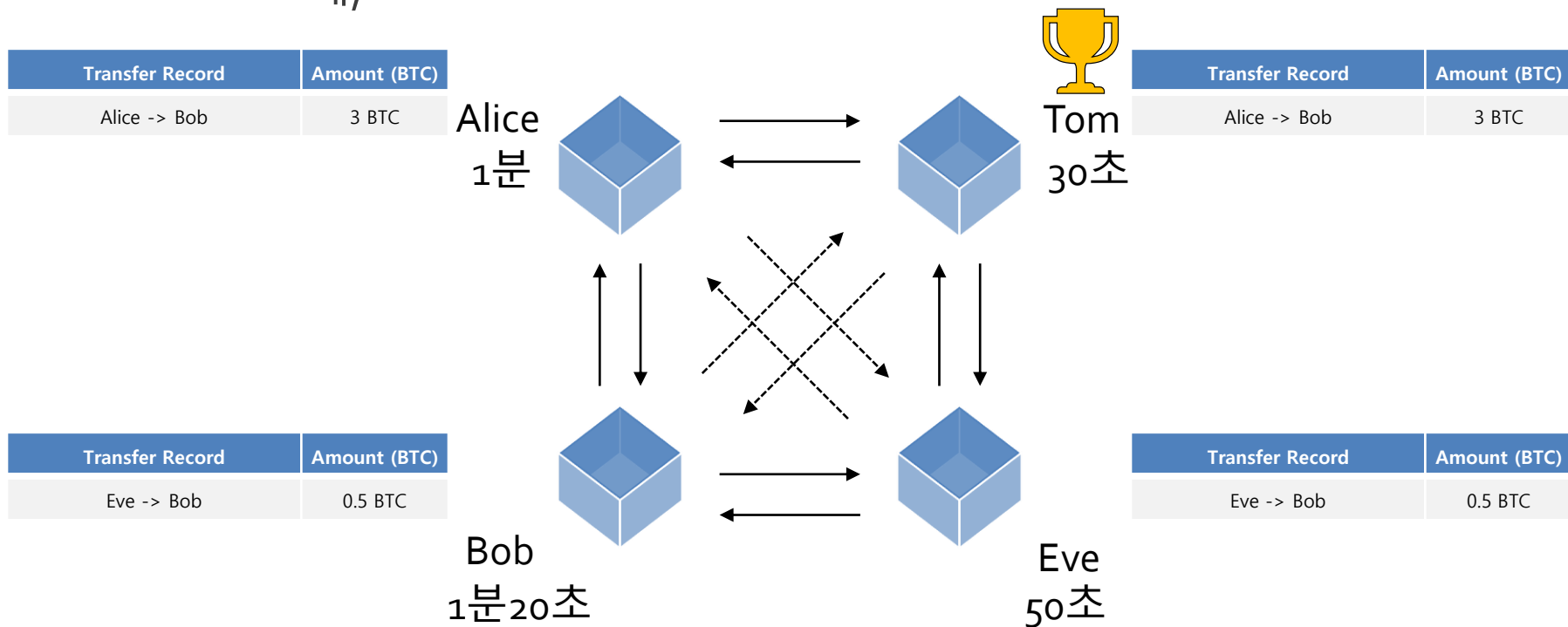
Hard problem

Introduction of Bitcoin

□ 비트코인 (Bitcoin)

▣ 합의 (Consensus)

- 모두가 이전 슬라이드에서의 스토쿠 문제를 풀어야 한다고 할 때,

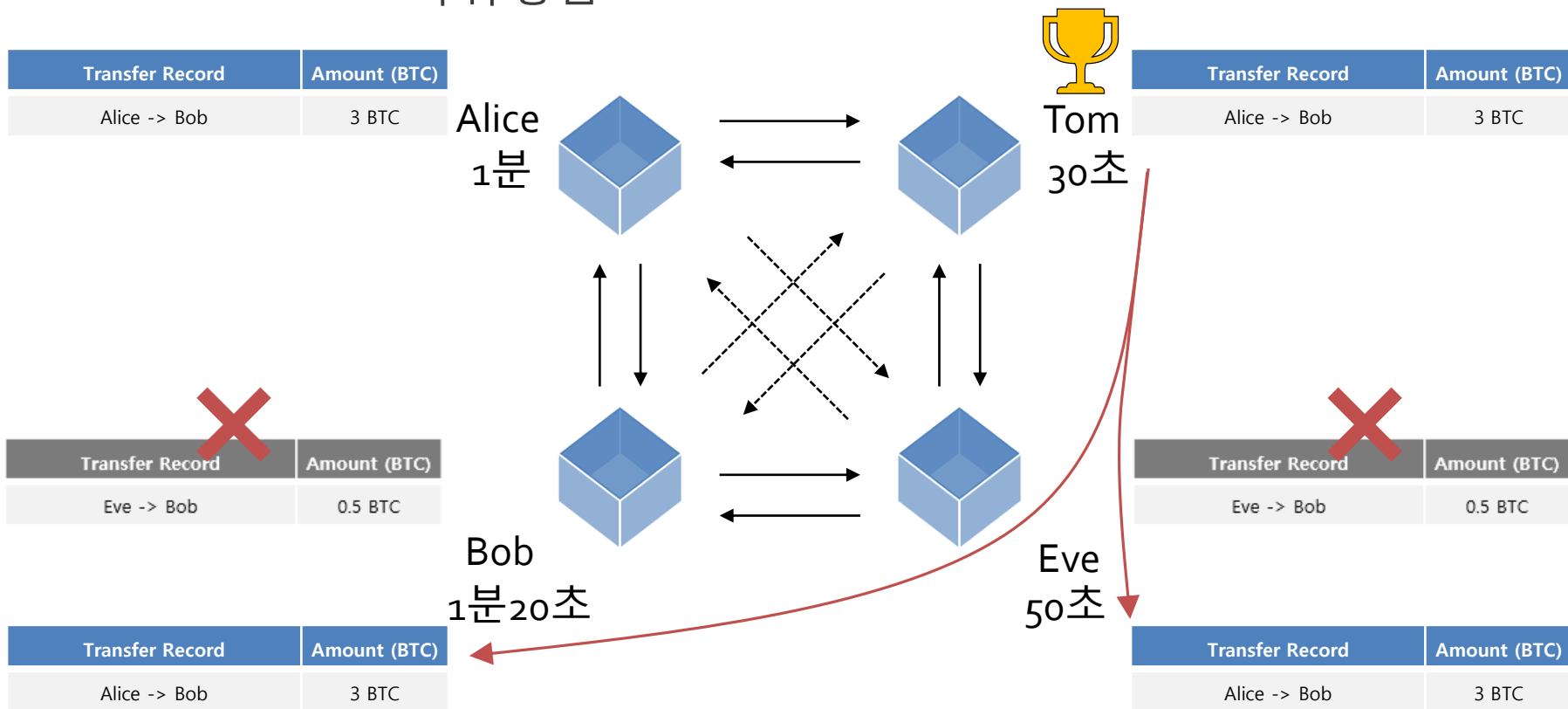


Introduction of Bitcoin

□ 비트코인 (Bitcoin)

▣ 합의 (Consensus)

- Bob, Eve는 자신들의 거래 데이터베이스를 Tom의 데이터 베이스로 바꿔 놓음



Introduction of Bitcoin

□ Summary

▣ 블록체인

- 블록체인의 정의 - P2P network 분산 데이터베이스 기반 저장 기술
- 블록체인의 역사 - Blind Signature, DigiCash, HashCash, Bit Gold, B-Mone, Bitcoin
- 블록체인의 기본 특징 - 분산원장, 암호화, 합의, 스마트 컨트랙트

▣ 비트코인

- 암호화폐
- 신원인증 - 공개키 (Public Key) 개인키 (Private Key)
- 기록 관리 - 모든 노드가 동일한 거래 기록을 분산하여 저장
- 합의 - 참여자들이 통일된 의사결정을 위해 사용 (PoW, PoS, ...)

- 블록체인

- Video link:

- <https://www.youtube.com/watch?v=cahoFr9cTn8>

- Lecture slides from BLOCKCHAIN @ BERKELEY

Q & A

