Blockchain #3

The basics of blockchain

Prof. Byung Il Kwak

Review

- 탈중앙화 시스템
  - 전자화폐의 추적 가능성
  - 이중 지불 문제
- 블록체인의 기본 특징
  - 분산원장, 암호화, 합의, 스마트 컨트랙트
- 암호화폐
  - 공개키 개인키를 이용한 신원 인증
  - 기록 관리와 합의 알고리즘 (Proof-of-Work)

CONTENTS

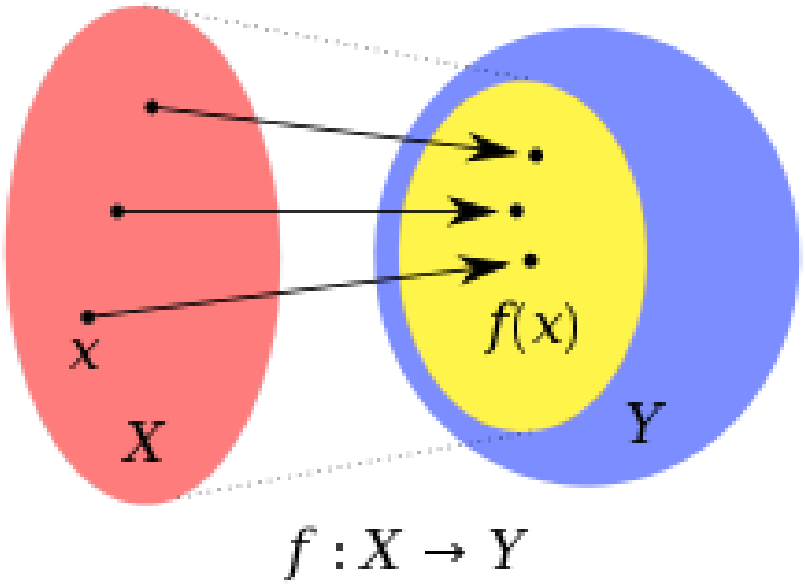
- Cryptography
  - Hash function
  - Digital signature

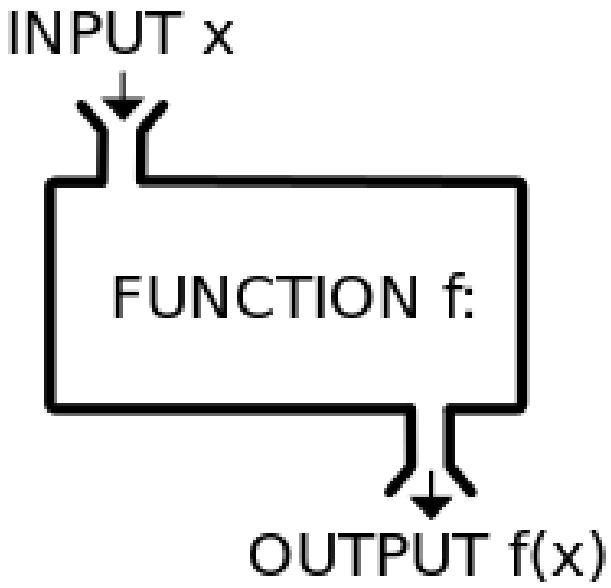
Cryptography - hash function

- 블록체인의 Trustless network
  - 제 3자에 대한 신용이 필요 없음
    - 은행과 같은 중앙에서 관리하는 특정 노드가 필요하지 않음
  - Trustless network에서의 신뢰성을 보장하기 위한 방법
    - Hash function을 활용한 암호화
    - 디지털 서명 (Public key & Private key)
    - 메시지 인증 코드 (Message authentication code algorithms)
    - …

Cryptography - hash function

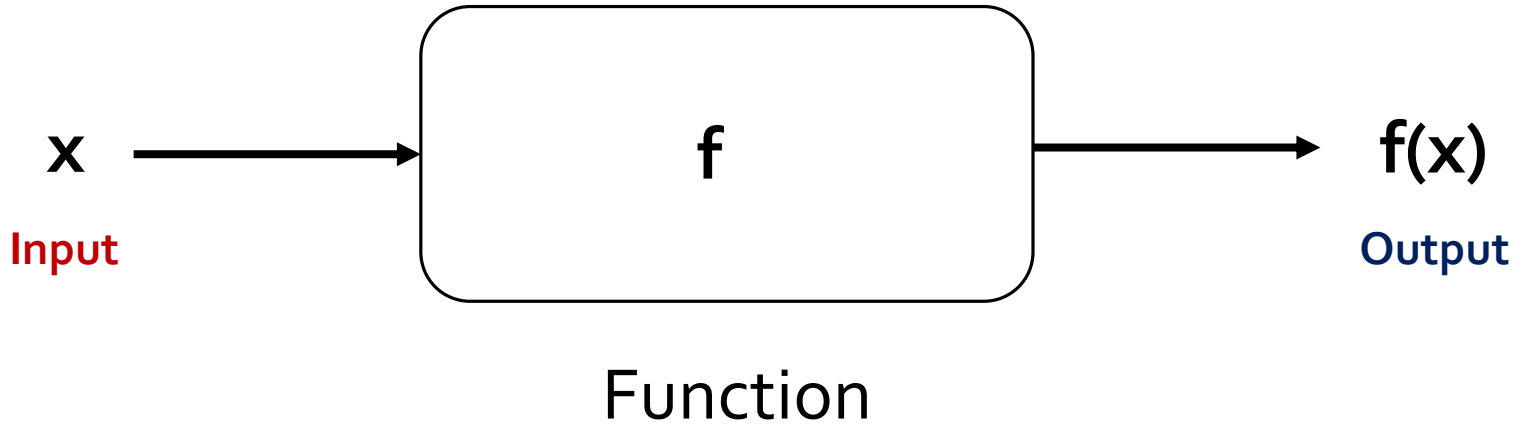
- 함수 (Function) 이란?





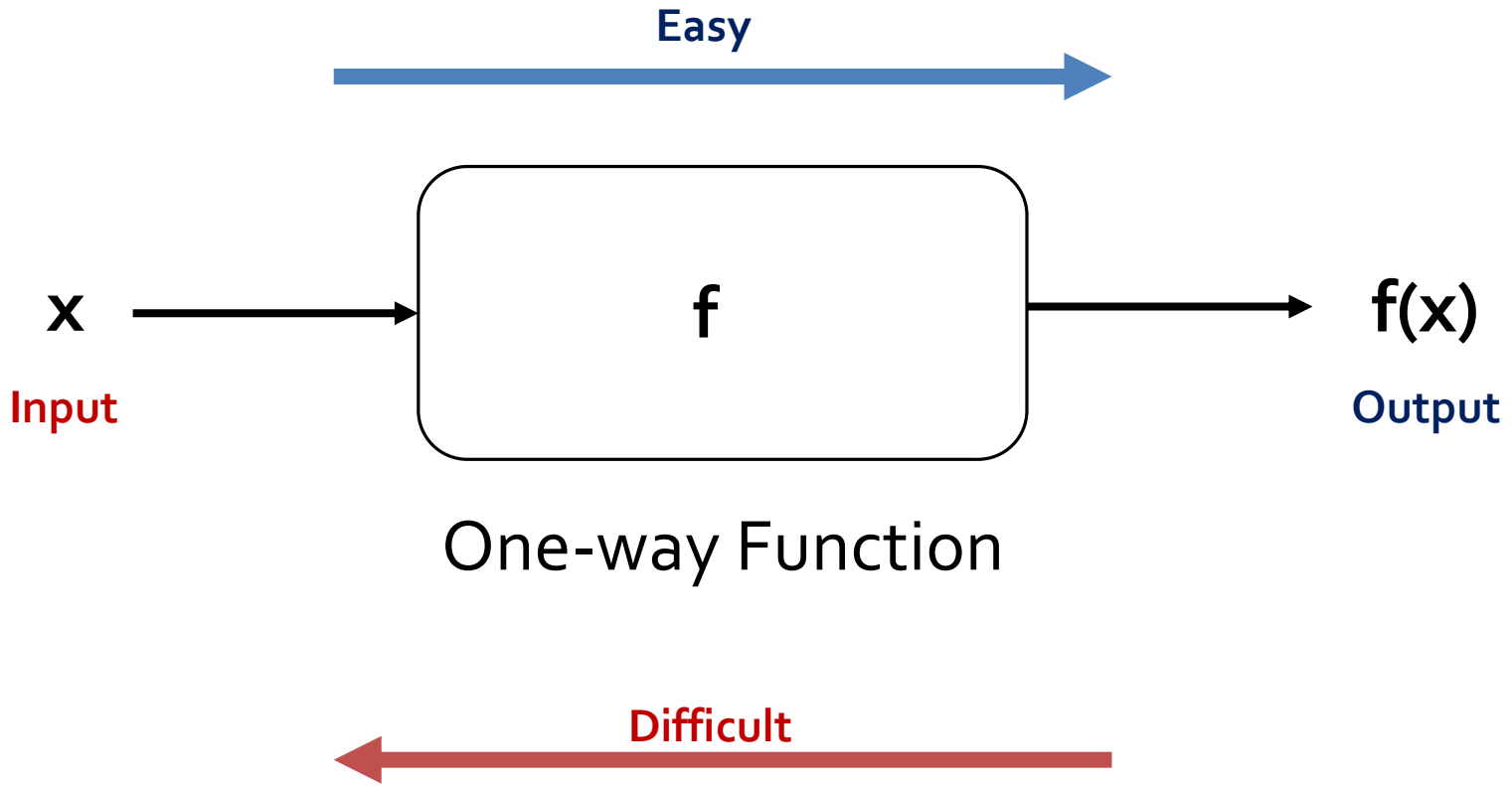
Cryptography - hash function

- 함수 (Function) 이란?



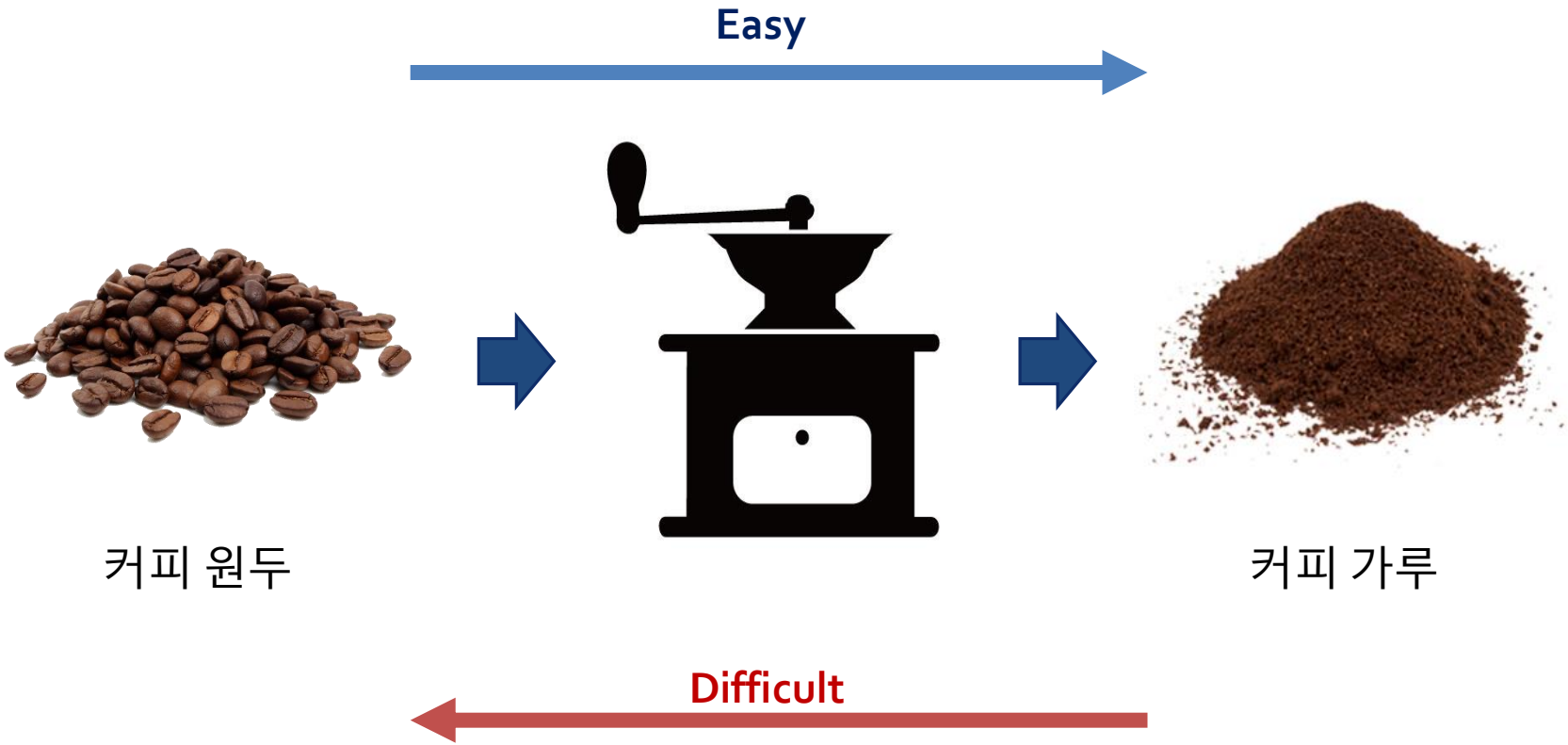
Cryptography - hash function

- 일 방향 함수 (One-way function) 이란?



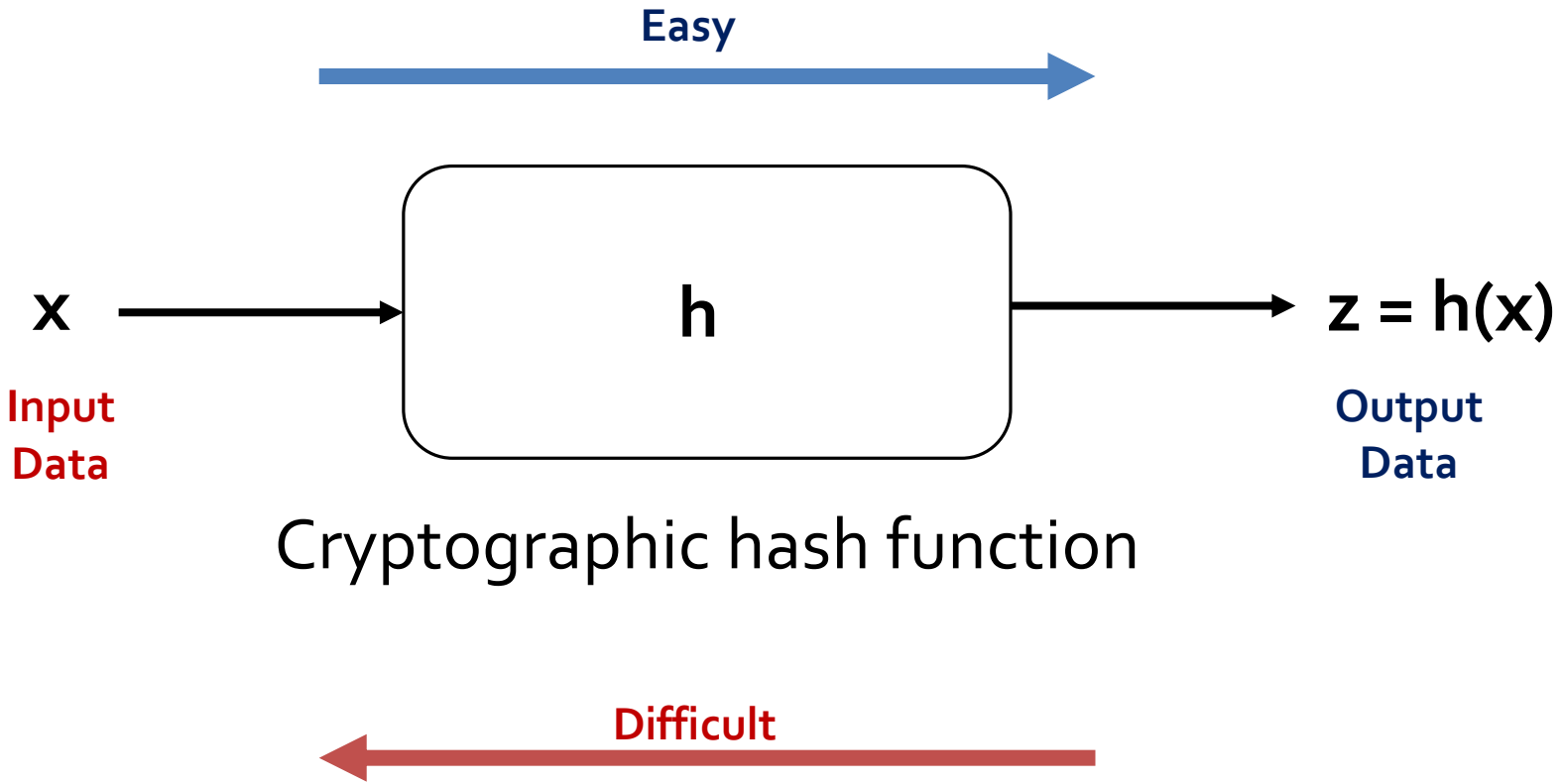
Cryptography - hash function

- 일 방향 함수 (One-way function) 예시



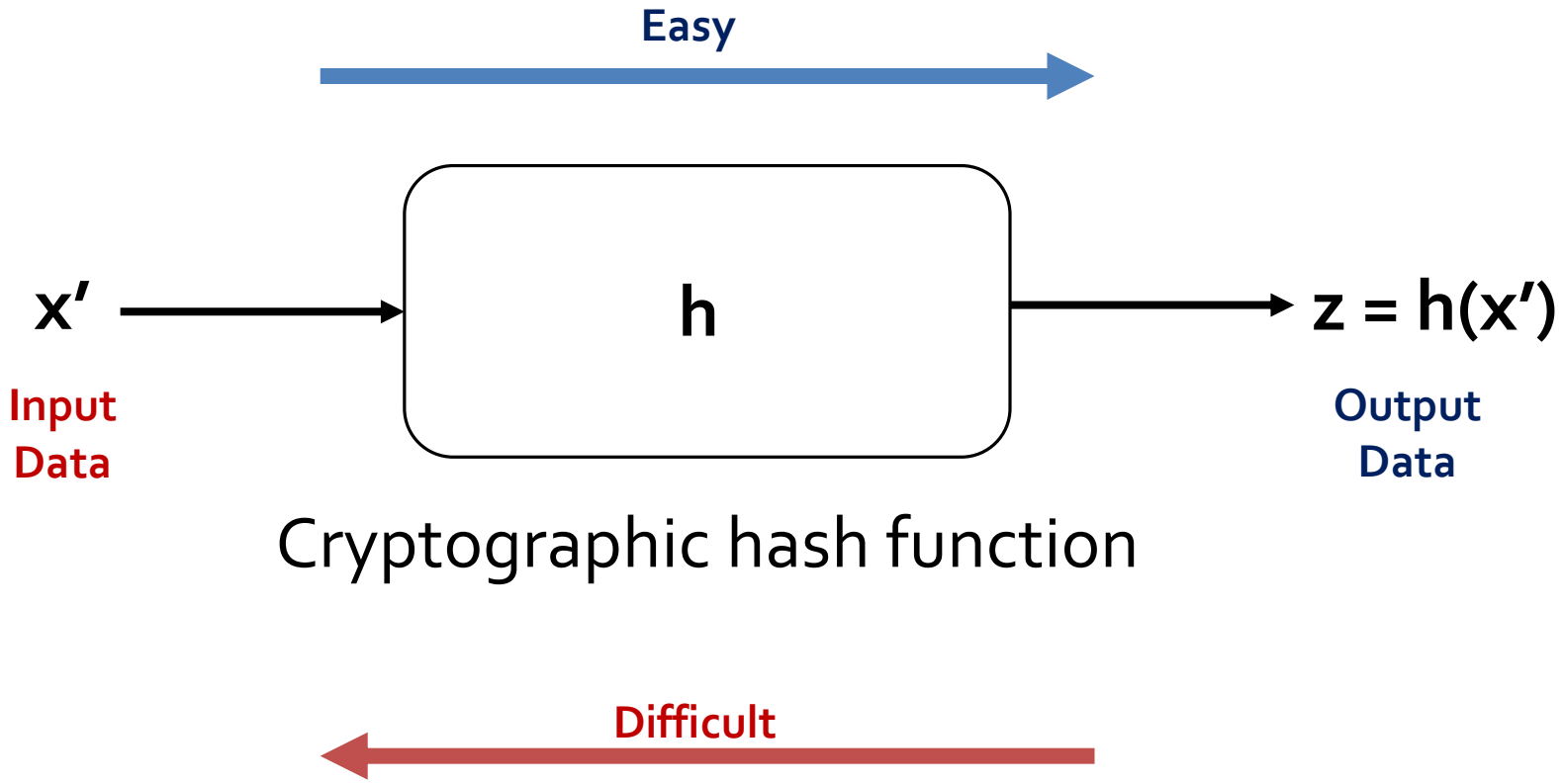
Cryptography - hash function

- Hash function (해시 함수)



Cryptography - hash function

- Hash function (해시 함수)



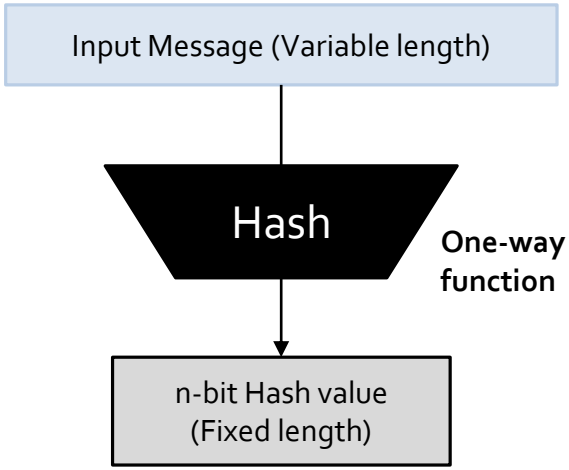
Cryptography - hash function

- Hash function (해시 함수)
  - Input data를 x, hash function 를 h, output을 z라고 할 때,
    - x는 z의 프리이미지 (preimage)라고도 함
    - z는 이미지 (image)라고 함
  - 이러한 경우, 해시 함수 h는 일대일의 함수가 아니기 때문에, 동일한 해시 값 z를 가질 수 있는 Input data x가 여러 개 존재할 수 있음

Cryptography - hash function

해시 함수의 조건

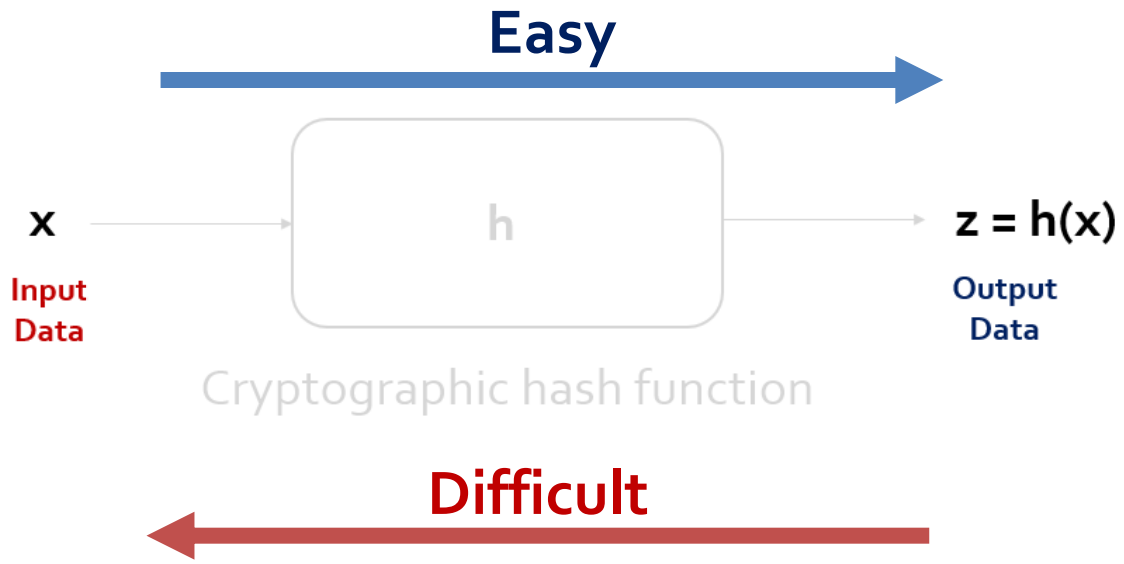
- ***Pre-image resistance:*** Given a hash value $\boldsymbol{h}$ it should be difficult to find any message $\boldsymbol{m}$ such that $\boldsymbol{h} = \boldsymbol{hash}(\boldsymbol{m})$
- ***Second pre-image resistance***: Given an input $\boldsymbol{m_1}$, it should be difficult to find a different input $\boldsymbol{m_2}$ such that $\boldsymbol{hash}(\boldsymbol{m_1}) = \boldsymbol{hash}(\boldsymbol{m_2})$
- ***Collision resistance:*** It should be difficult to find two different messages $\boldsymbol{m_1}$ and $\boldsymbol{m_2}$ such that $\boldsymbol{hash}(\boldsymbol{m_1}) = \boldsymbol{hash}(\boldsymbol{m_2})$



- 해시 함수는 'Digital fingerprints (디지털 지문)'으로도 사용됨

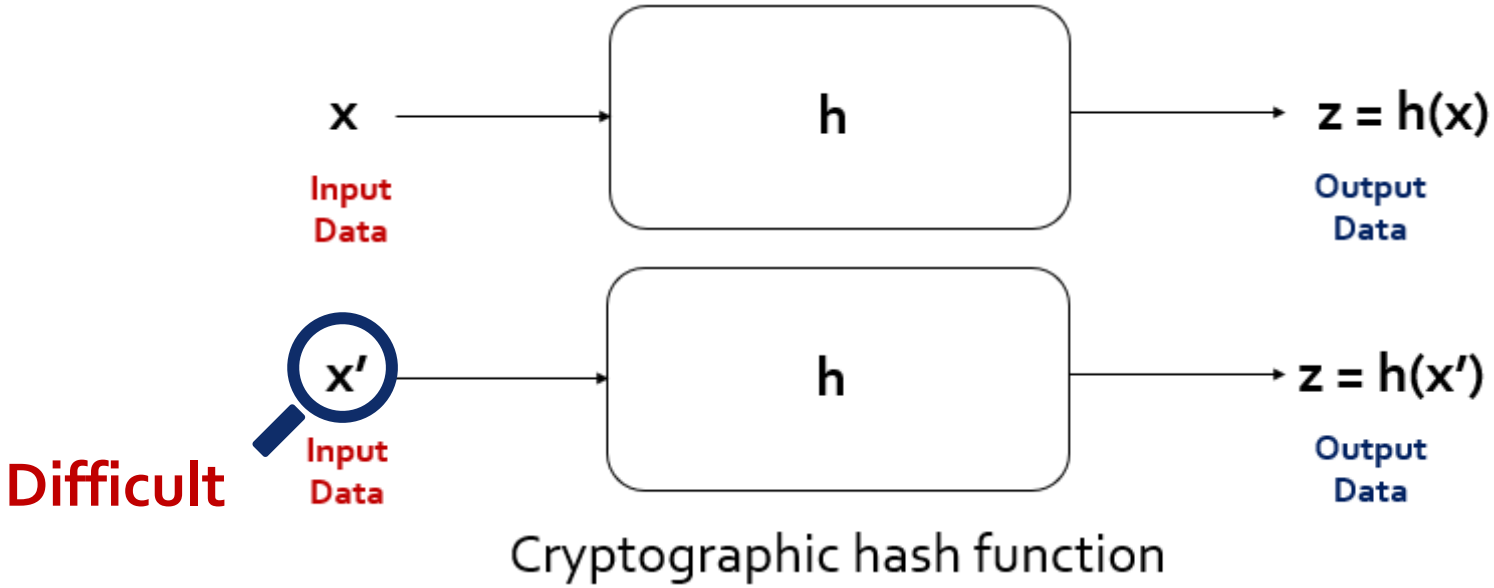
Cryptography - hash function

- 해시 함수의 조건
  - 프리 이미지 저항성 (Preimage resistance)
    - 해시 값 z로 문서 x를 찾는 것이 어려워야 함
    - 해시의 단방향적 성질을 의미
      - 주어진 z를 통해 x를 찾는 것은 어려움



Cryptography - hash function

- 해시 함수의 조건
  - 제 2 프리 이미지 저항성 (Second preimage resistance)
    - Input Data x가 주어졌을 때, 해시 값 z를 갖는 또 다른 Input Data x′의 발견이 어려워야 함
      - 주어진 x, z에 대해, x를 h()에 적용한 z = h(x)가 있을 경우, z = h(x) = h(x′) 인 x′를 찾기가 어려워함

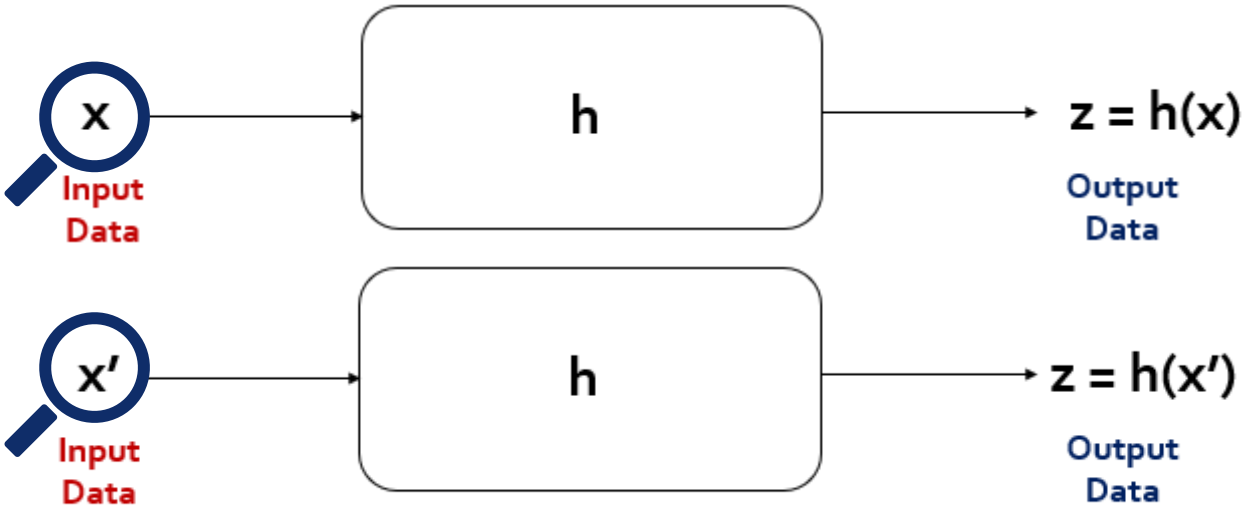


Cryptographic hash function

Cryptography - hash function

- 해시 함수의 조건
  - 충돌 저항성 (Collision resistance)
    - 동일한 해시 값 z를 갖는 임의의 두 Input Data x, x′을 찾는 것이 어려워야 함
      - 주어진 정보가 없을 때, 해시 값 z에 대한 h(x) = h(x′) = z를 만족하는 (x, x′)을 찾는 것이 어려워야 함

Difficult



Cryptographic hash function

Cryptography - hash function

- 해시 함수
  - 눈사태 효과 (Avalanche effect)
    - 암호 알고리즘에서 입력 값에 미세한 변화를 줄 경우 출력 값에 상당한 변화가 일어나는 성질 [source: *Wikipedia]*
    - 해시 함수에서의 눈사태 효과 (Avalanche effect)
      - 해시 함수에서 Input Data가 1 bit만 차이를 보여도 Output Data는 다르게 나타남

Hash Algorithm Types	Input Data	Hash values
SHA1	1	356A192B7913B04C54574D18C28D46E6395428AB
	2	DA4B9237BACCCDF19C0760CAB7AEC4A8359010B0
	3	77DE68DAECD823BABBB58EDB1C8E14D7106E83BB
	4	1B6453892473A467D07372D45EB05ABC2031647A

Cryptography - hash function

- 해시 함수
  - 눈사태 효과 (Avalanche effect)

```
I am Satoshi Nakamoto0 => a80a81401765c8eddee25df36728d732...
I am Satoshi Nakamoto1 => f7bc9a6304a4647bb41241a677b5345f...
I am Satoshi Nakamoto2 => ea758a8134b115298a1583ffb80ae629...
I am Satoshi Nakamoto3 => bfa9779618ff072c903d773de30c99bd...
I am Satoshi Nakamoto4 => bce8564de9a83c18c31944a66bde992f...
I am Satoshi Nakamoto5 => eb362c3cf3479be0a97a20163589038e...
I am Satoshi Nakamoto6 => 4a2fd48e3be420d0d28e202360cfbaba...
I am Satoshi Nakamoto7 => 790b5a1349a5f2b909bf74d0d166b17a...
I am Satoshi Nakamoto8 => 702c45e5b15aa54b625d68dd947f1597...
I am Satoshi Nakamoto9 => 7007cf7dd40f5e933cd89fff5b791ff0...
I am Satoshi Nakamoto10 => c2f38c81992f4614206a21537bd634a...
I am Satoshi Nakamoto11 => 7045da6ed8a914690f087690e1e8d66...
I am Satoshi Nakamoto12 => 60f01db30c1a0d4cbce2b4b22e88b9b...
I am Satoshi Nakamoto13 => 0ebc56d59a34f5082aaef3d66b37a66...
I am Satoshi Nakamoto14 => 27ead1ca85da66981fd9da01a8c6816...
I am Satoshi Nakamoto15 => 394809fb809c5f83ce97ab554a2812c...
I am Satoshi Nakamoto16 => 8fa4992219df33f50834465d3047429...
I am Satoshi Nakamoto17 => dca9b8b4f8d8e1521fa4eaa46f4f0cd...
I am Satoshi Nakamoto18 => 9989a401b2a3a318b01e9ca9a22b0f3...
I am Satoshi Nakamoto19 => cda56022ecb5b67b2bc93a2d764e75f...
```

[Source: http://chimera.labs.oreilly.com/books/1234000001802/ch08.html#_proof_of_work_algorithm]

SHA: Secure Hash Algorithm

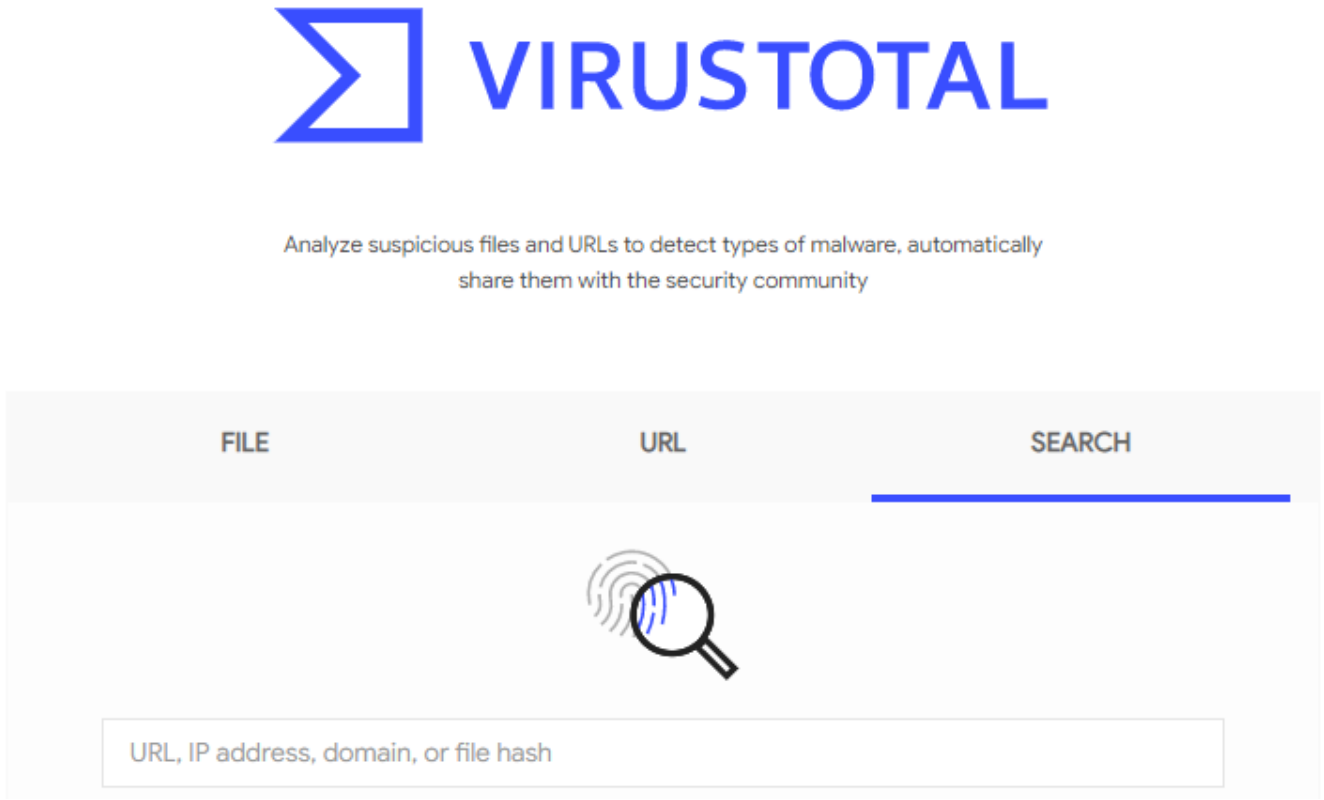
https://passwordsgenerator.net/sha1-hash-generator/

Cryptography - hash function

- 해시 알고리즘 종류
  - MD5: 1991. Rivest개발, 128비트 알고리즘
  - SHA-1: 1995. 미국 NIST 표준 채택, 160비트 알고리즘
  - RIPEMD160: 1996. Han Dobbertin 개발, 160비트 알고리즘
  - SHA-256, 384, 512: 2002. 미국 NIST 표준 채택, 256, 384, 512 비트 알고리즘
  - MD5, SHA-1은 충돌 저항성이 낮음
  - 현재에는 SHA-256이 널리 사용됨

Cryptography - hash function

- 해시 함수 사용 케이스



https://support.virustotal.com/hc/en-us/articles/115002739245-Searching

Cryptography - hash function

- 해시 함수 사용 케이스

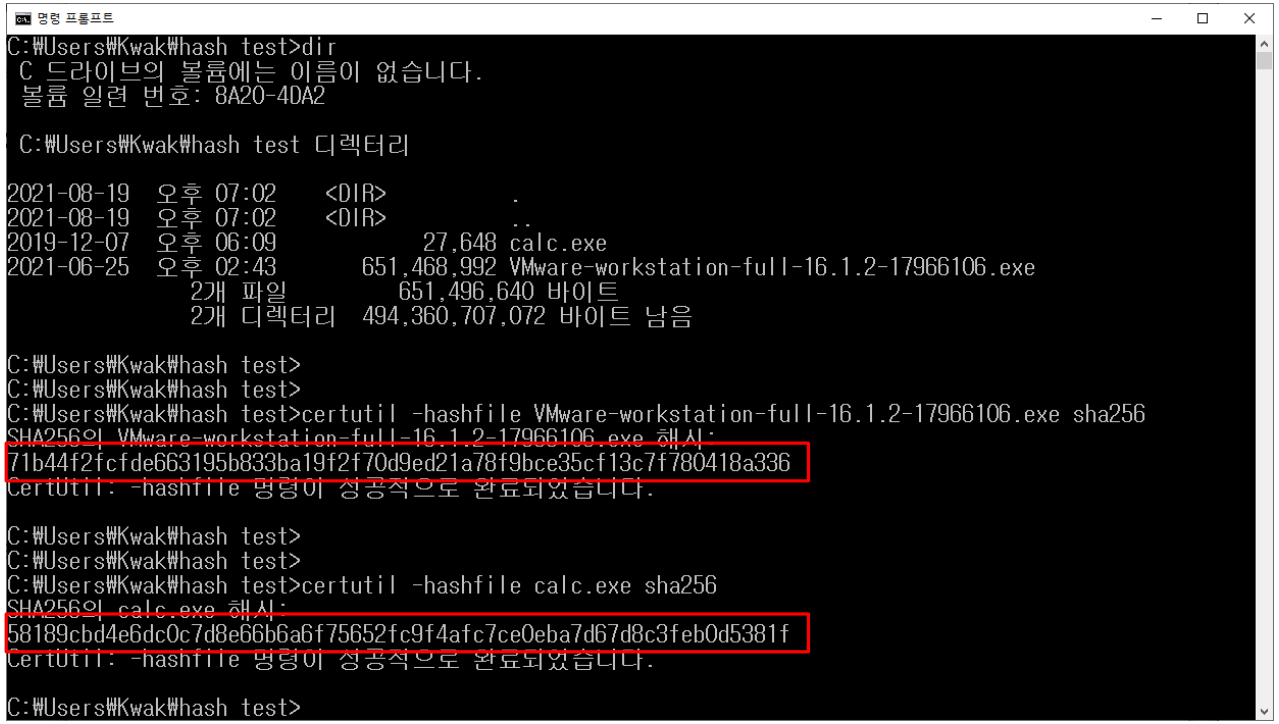
Download Kali Linux Images

We generate fresh Kali Linux image files every few months, which we make available for download. This page provides the links to **download Kali Linux** in its latest official release. For a release history, check our Kali Linux Releases page. Please note: You can find unofficial, untested weekly releases at http://cdimage.kali.org/kali-weekly/.

Image Name	Download	Size	Version	sha256sum
Kali Linux 64 Bit	HTTP | Torrent	2.8G	2018.2	56f677e2edfb2efcd0b08662ddde824e254c3d53567ebbbcdbbf5c03efd9bc0f
Kali Linux Light 64 Bit	HTTP | Torrent	865M	2018.2	554f020b0c89d5978928d31b8635a7eeddf0a3900abcacdbc39616f80d247f86
Kali Linux E17 64 Bit	HTTP | Torrent	2.6G	2018.2	be0a858c4a1862eb5d7b8875852e7d38ef852c335c3c23852a8b08807b4c3be8
Kali Linux Lxde 64 Bit	HTTP | Torrent	2.6G	2018.2	449ecca86b0f49a52f95a51acdde94745821020b7fc0bd2129628c56bc2d145d
Kali Linux Xfce 64 Bit	HTTP | Torrent	2.6G	2018.2	0e94035a0a56fccc49961b0da56b9243ed3da6a3f8d696884e6f0b936f74dbfb

Cryptography - hash function

- 해시 함수 사용 케이스



  - 윈도우 cmd
    - > certutil -hashfile 파일명 해시알고리즘
      - MD2, MD4, MD5, SHA1, SHA256, SHA384, SHA512

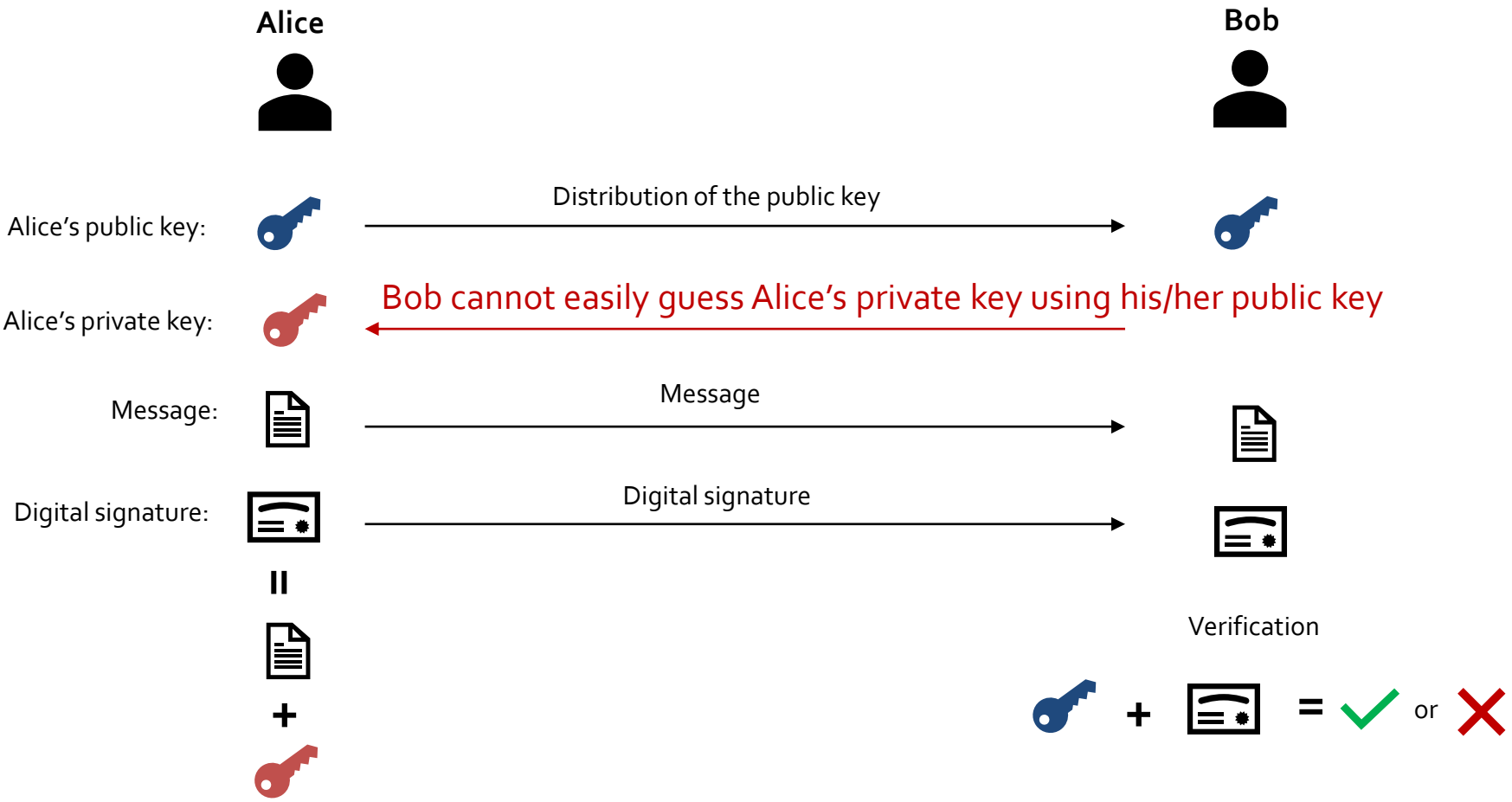
Cryptography - digital signature

- 전자 서명 (Digital signature)
  - 인증 (Authentication)
    - 전자 서명을 통해 서명자를 검증할 수 있음
  - 메시지 무결성 (Integrity)
    - 메시지는 서명 후에 변경될 수 없음
  - 부인방지 (Non-repudiation)
    - 발신자는 서명한 사실을 부인할 수 없음
  - 전자 서명 알고리즘의 종류
    - RSA, ECDSA, …

RSA: MIT's Rivest, Shamir and Adleman
ECDSA: Elliptic Curve Digital Signature Algorithm

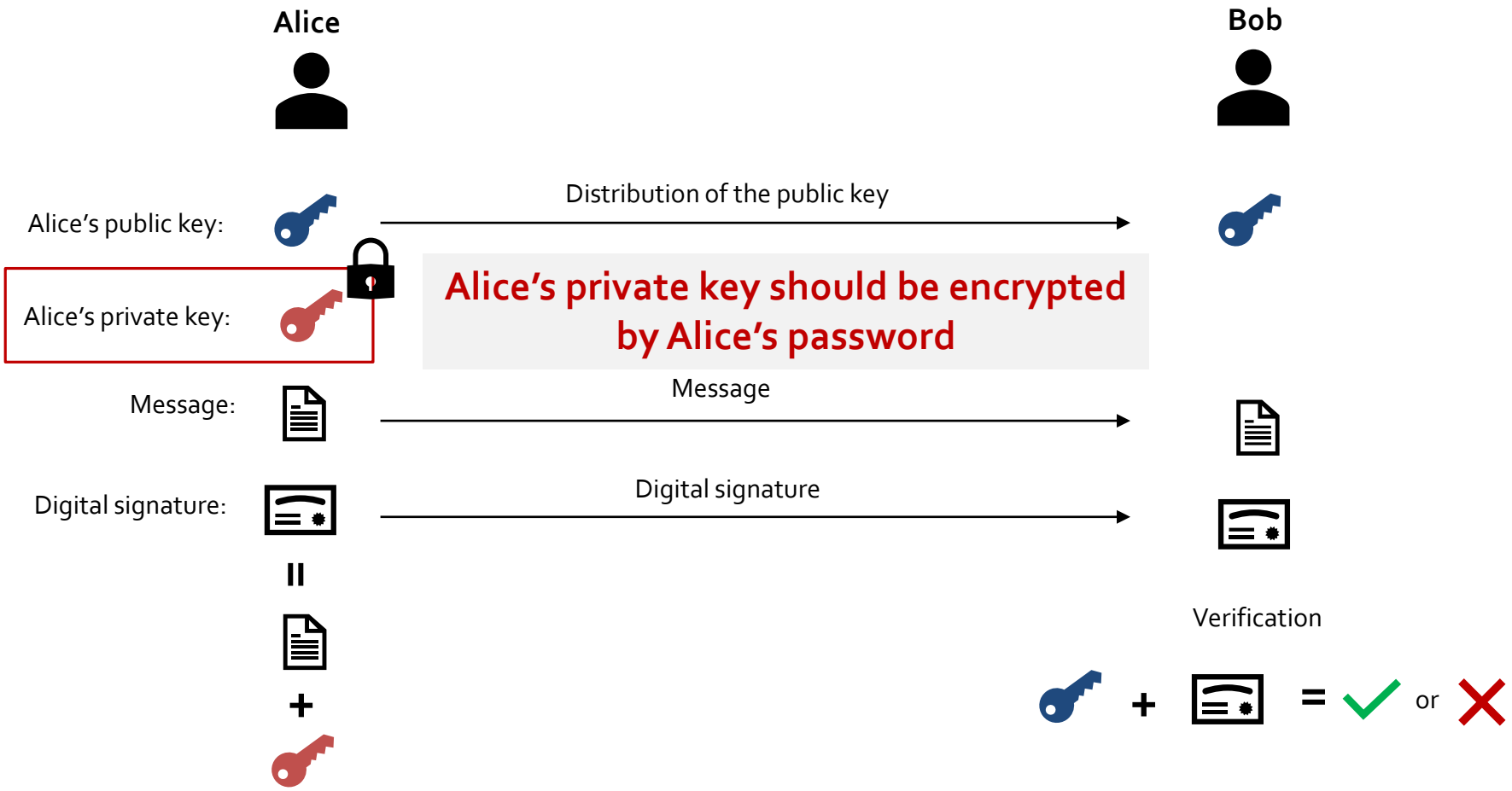
Cryptography - digital signature

- 전자 서명 (Digital signature) 기본 개념 및 흐름



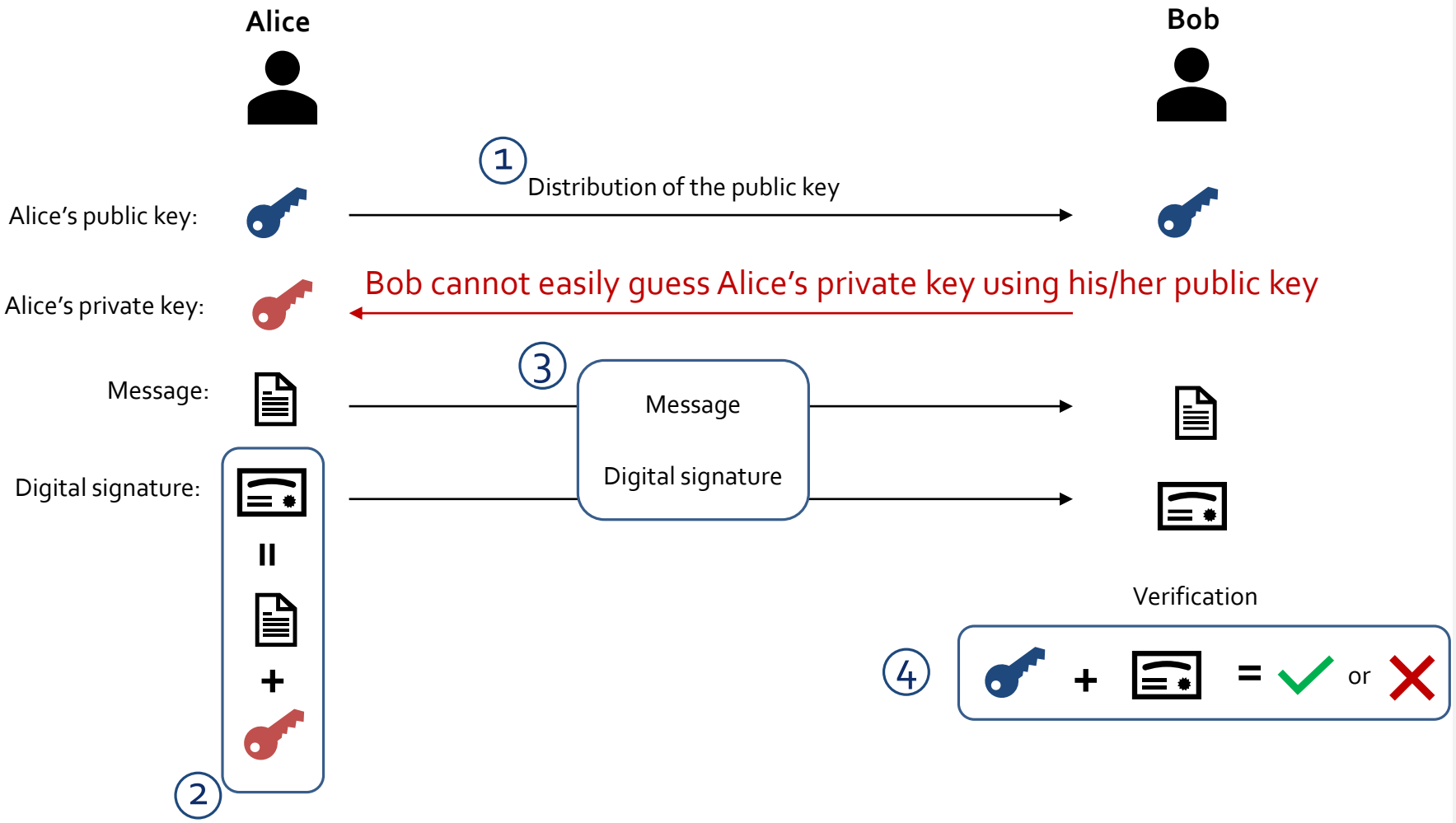
Cryptography - digital signature

- 전자 서명 (Digital signature) 기본 개념 및 흐름



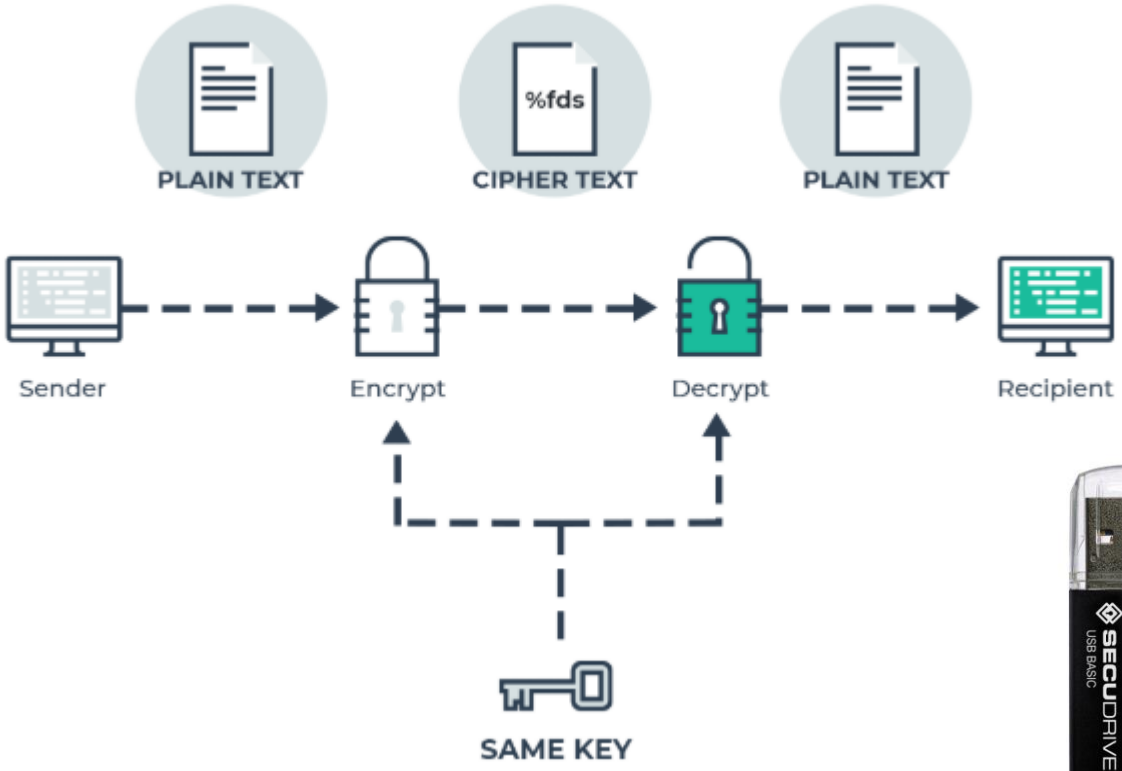
Cryptography - digital signature

- 전자 서명 (Digital signature) 기본 개념 및 흐름



Appendix. Encryption

- (Symmetric) Encryption (e.g., AES)

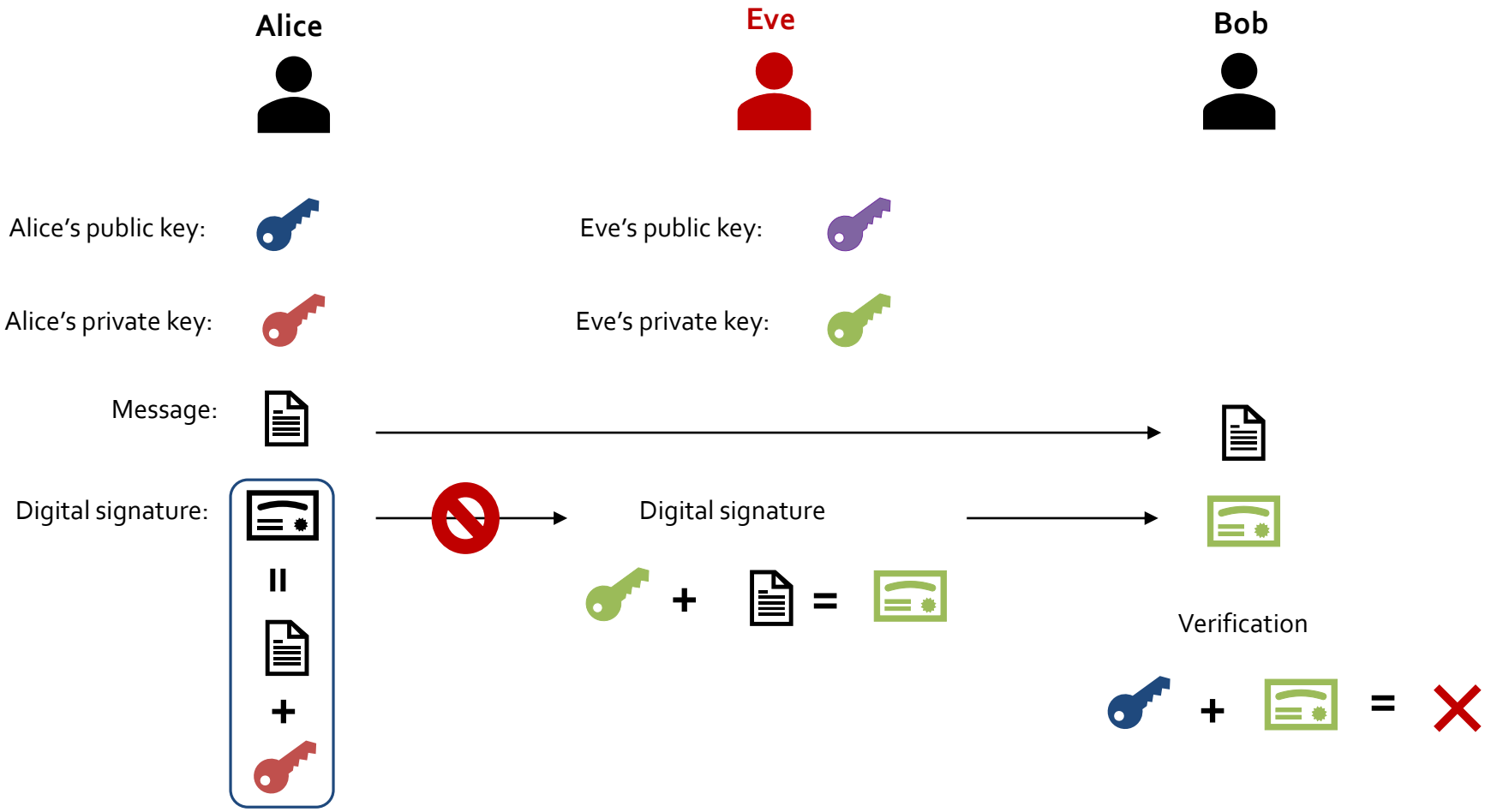


[Source: https://pixelprivacy.com/resources/what-is-encryption/]

AES: Advanced Encryption Standard

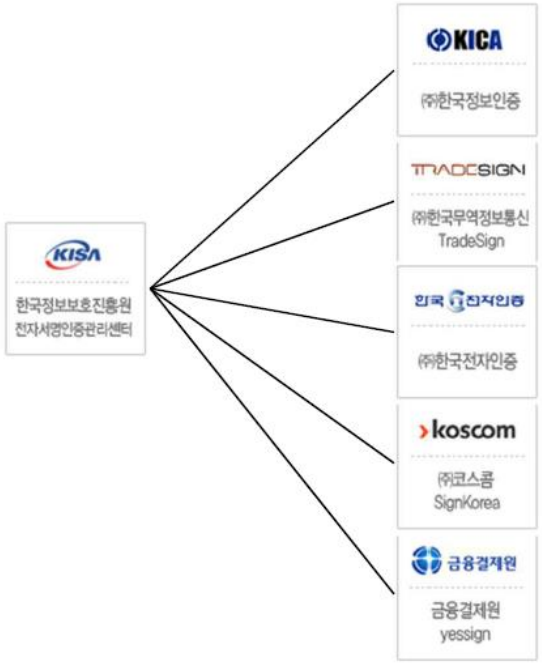
Cryptography - digital signature

- 전자 서명 (Digital signature) 기본 개념 및 흐름



Cryptography - digital signature

- 공개키 기반의 전자서명 활용



공인인증기관

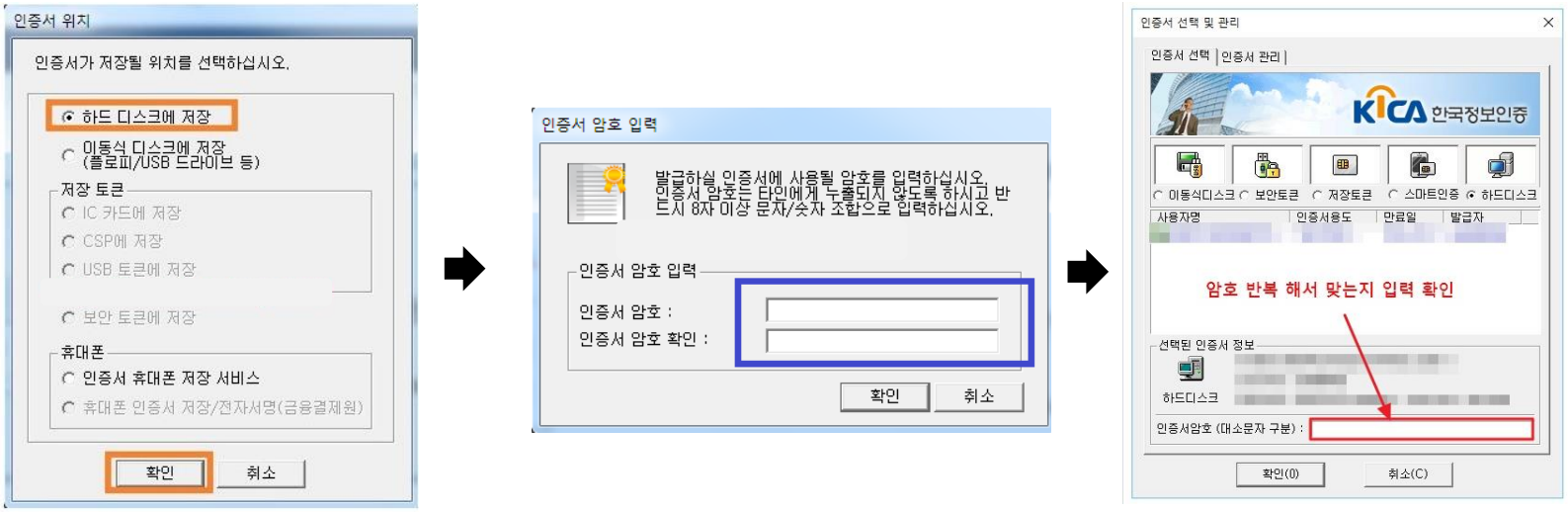
공인인증서의 용도 [편집]

대구분	소구분	용도	관련사이트
금융	인터넷뱅킹	인터넷뱅킹 홈페이지 로그인 및 계좌이체	
	온라인증권거래	온라인증권거래(HTS) 로그인 및 증권매도/매수 주문	
	신용카드 결제	쇼핑몰 등에서 신용카드 온라인 결제(30만원 이상은 의무사용)	
	보험업무	온라인 보험 가입 또는 관련 증명서 발급	
	지로납부	지로요금, 공과금, 범칙금, 세금 납부	http://www.giro.or.kr
기업전자상거래 (B2B)	입찰	온라인 입찰서 제출 (조달청, 공공기관, 대기업 등)	http://www.certbiz.com
	계약	온라인 계약서 작성 및 승인	http://www.certbiz.com
	세금계산서	매출세금계산서 작성 및 승인	http://www.certbiz.com
민원업무(공공/행정)	실적신고	건설협회, 화학물질관리협회 등의 온라인 실적신고	
	증명서발급	건설협회, 무역협회 등의 온라인 증명서 발급업무	
부동산	아파트 온라인 청약	공공, 민영 아파트 인터넷 청약	
의료	전자처방전, 전자의무행정		
정부민원업무	대한민국전자정부포탈	정부민원업무 포탈서비스	http://gov.kr
정부민원업무	헌법재판소 전자헌법재판센터	전자접수, 전자송달	http://ecourt.ccourt.go.kr
정부민원업무	대법원 인터넷등기소	부동산등기, 법인등기	http://www.iros.go.kr
정부민원업무	대법원 가족관계등록시스템	가족관계등록부 발급(가족관계증명서, 기본증명서 등)	https://efamily.scourt.go.kr
정부민원업무	국세청 홈택스	국세납부, 연말정산 등	http://www.hometax.go.kr
정부민원업무	관세청 인터넷통관포탈	수출입통관, 관세환급, 요건확인	http://portal.customs.go.kr
정부민원업무	행정안전부 정부24	토지대장열람, 주민등록등초본교부, 건축물대장 등초본교부, 전입신고 등	http://gov.kr

https://ko.wikipedia.org/wiki/공동인증서

Cryptography - digital signature

- 공개키 기반의 전자서명 활용
  - 인증서에는 사용자의 공개키가 탑재됨
  - 해당 인증서 (공개 키)는 어떤 곳이든 저장하고 관리할 수 있음
  - 하지만, 개인 키는 암호화되어 사용자의 개인 저장소에 저장되어야 함

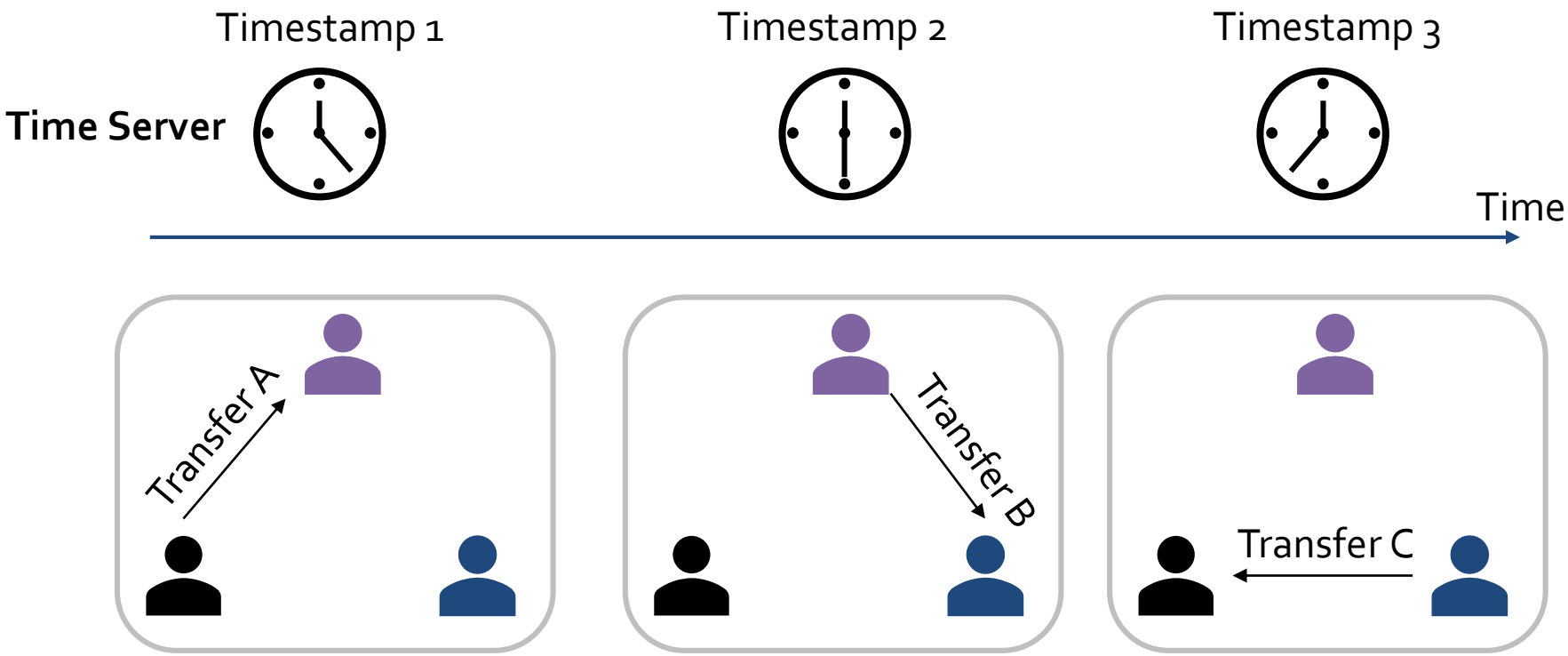


CONTENTS

- Time synchronization on decentralized networks

Time synchronization

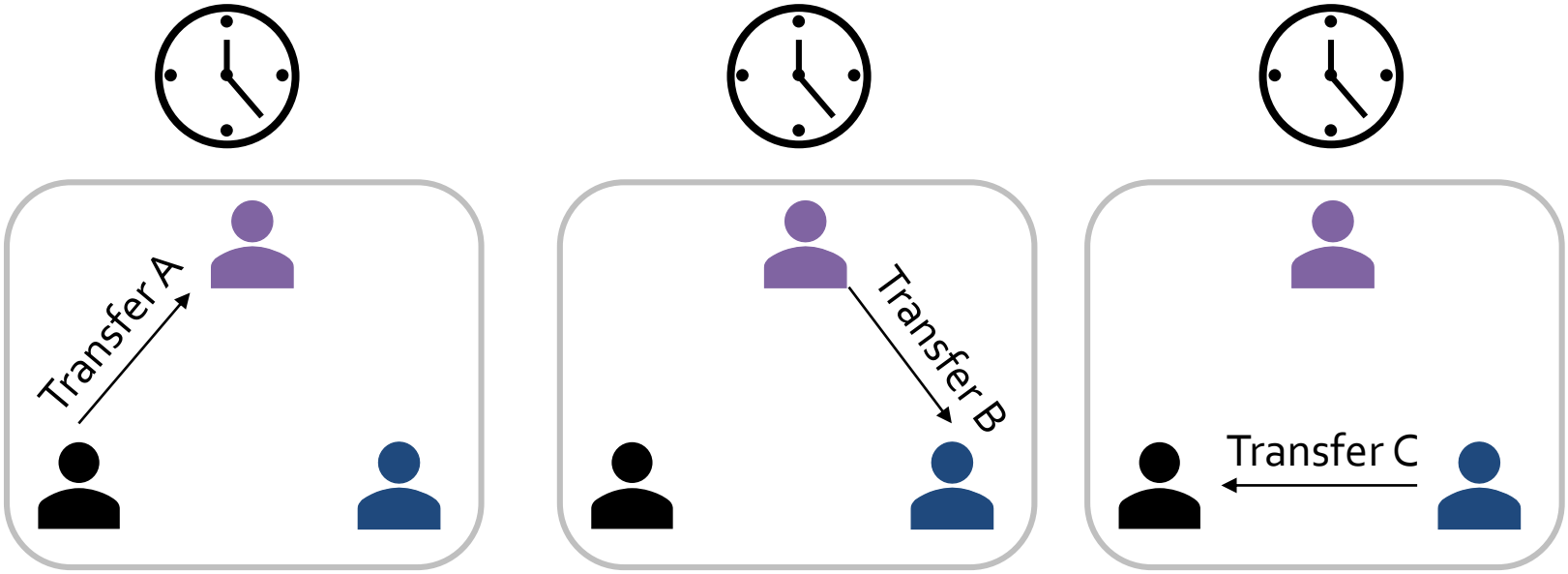
- 중앙 서버에 의한 Timestamp



Event sequence: Transfer A → Transfer B → Transfer C

Time synchronization

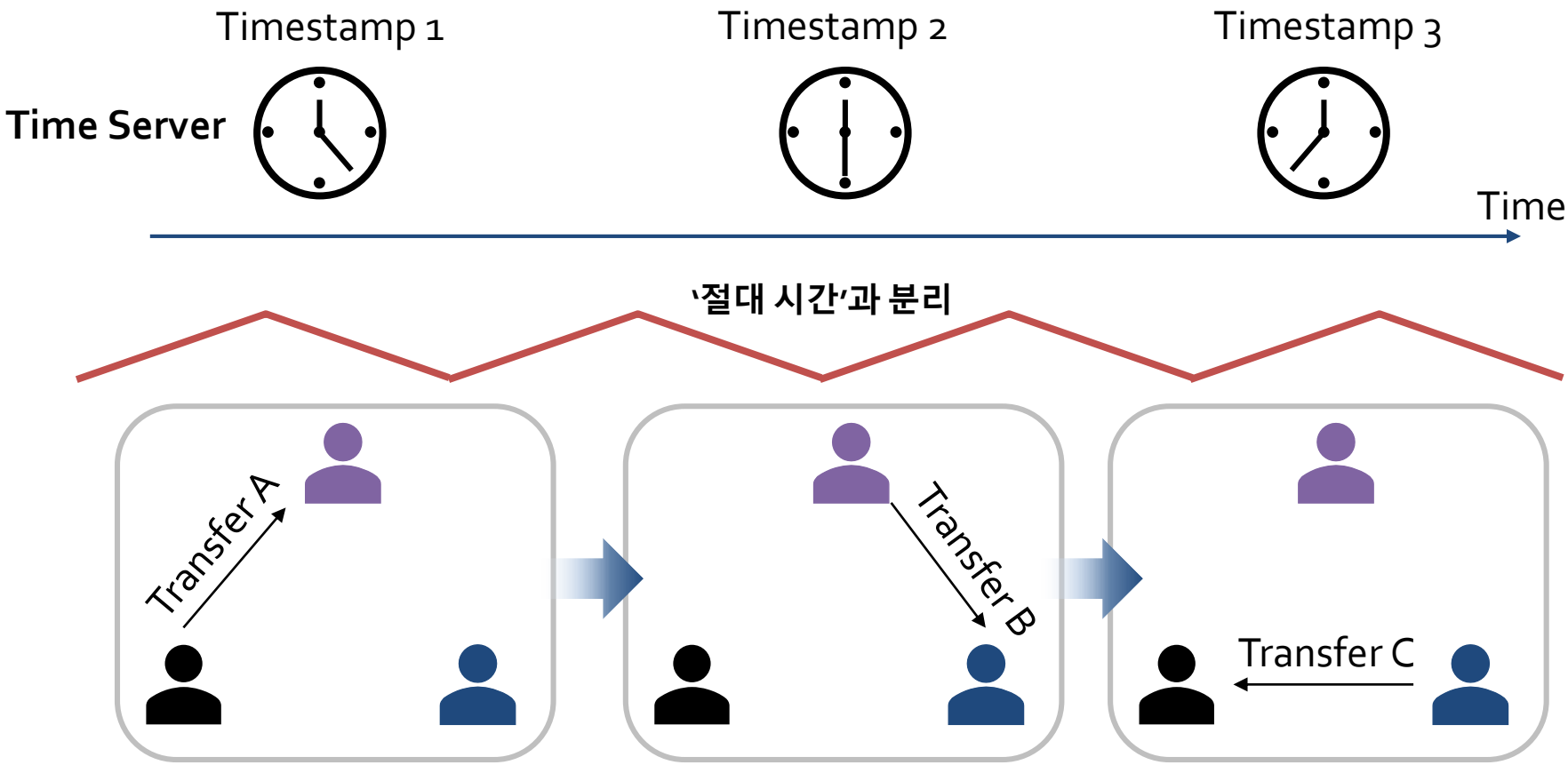
- 중앙 서버가 없을 경우의 Timestamp
  - 기준이 되는 Timestamp가 사라짐



Event sequence: *Transfer A ? Transfer B ? Transfer C*

Time synchronization

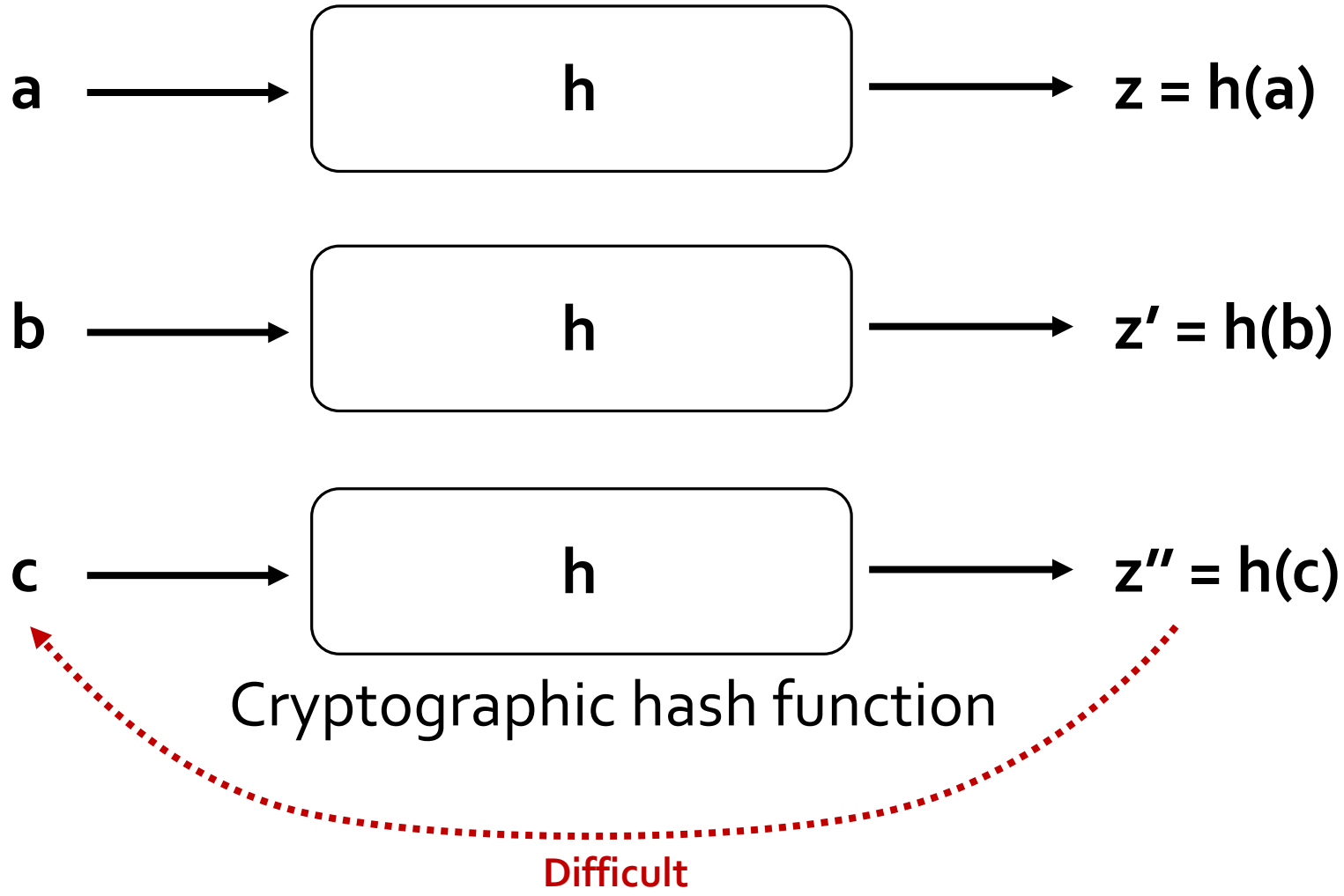
- 중앙 서버가 없을 경우의 Timestamp



Event sequence: Transfer A → Transfer B → Transfer C

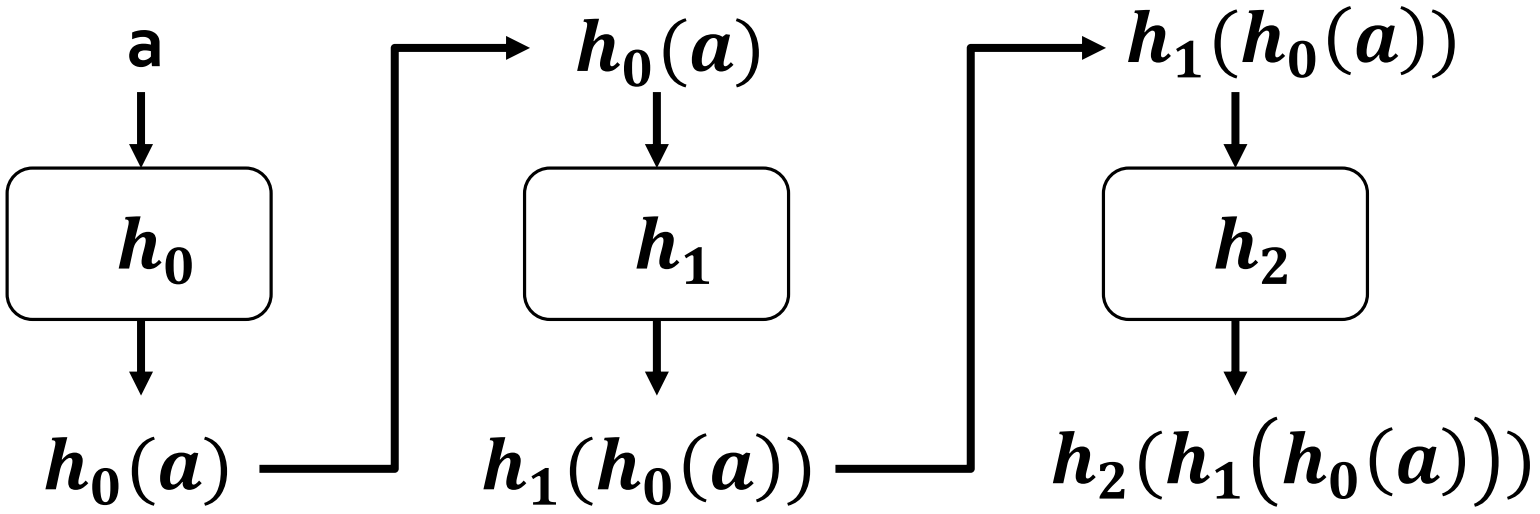
Time synchronization

- 중앙 서버가 없을 경우? **Hash-chain**



Time synchronization

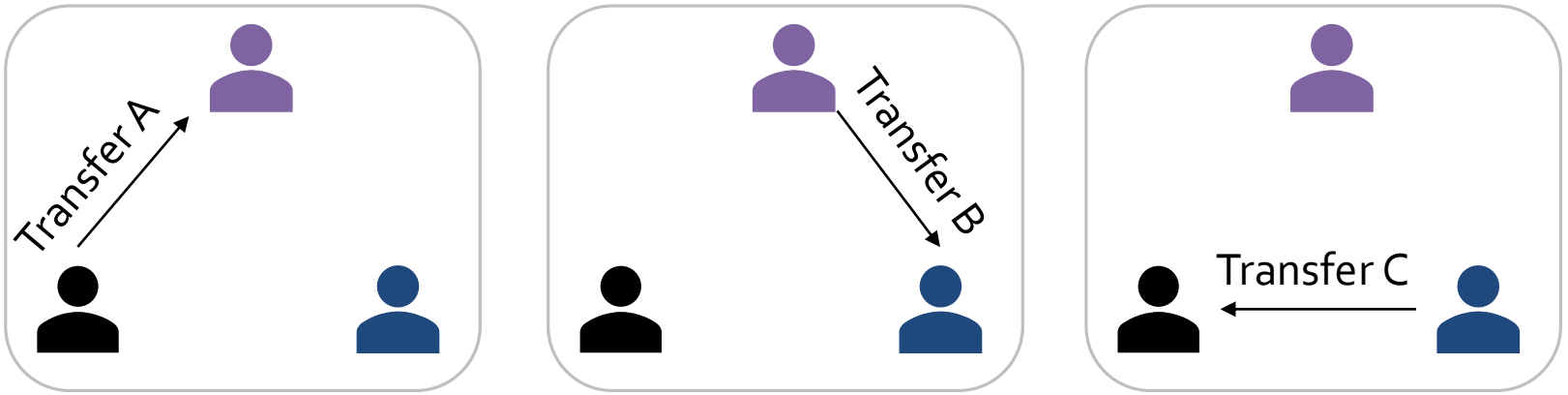
- Hash-chain 활용



Hash-chain: h_0 -> h_1 -> h_2

Time synchronization

- Hash-chain 활용한 탈중앙화 타임 스탬프



$h_0 = H(Transfer\ A)$ $h_1 = H(h_0||Transfer\ B)$ $h_2 = H(h_1||Transfer\ C)$

Event sequence: Transfer A → Transfer B → Transfer C

CONTENTS

- Blockchain Details
  - Blockchain (Generation and chaining blocks)
  - Openness (Public and private)
  - Consensus (Fork, consensus models)

Blockchain Details

거래 생성 (Transaction generation)

1. Alice generates transaction data ($Trans_{Alcie}$)

Example of transaction

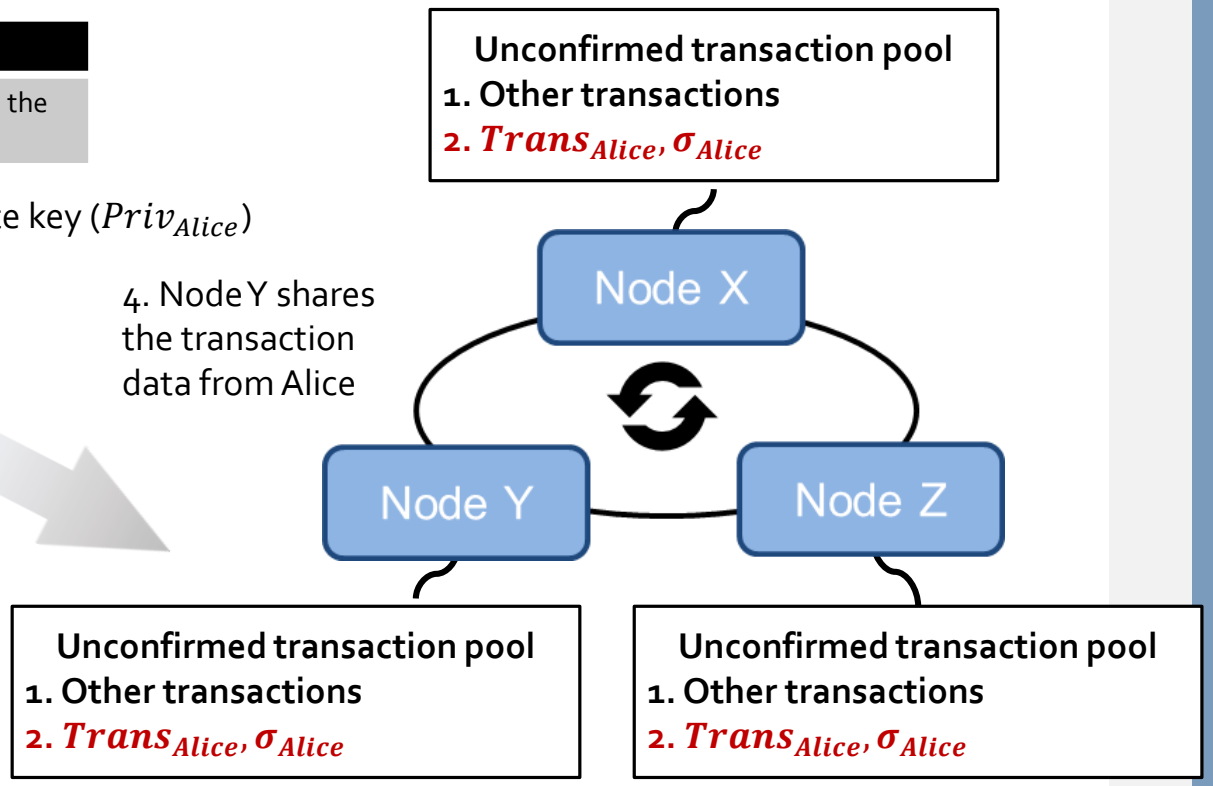
From	To	Contents
Alice	Bob	Move a pawn to the position X

2. Alice signs $Trans_{Alcie}$ using Alice's private key ($Priv_{Alice}$)
($\sigma_{Alice} = Sign_{Priv_{Alice}}(Trans_{Alice})$)

Alice

3. Alice sends transaction data to one node of blockchain network (e.g., Node Y)

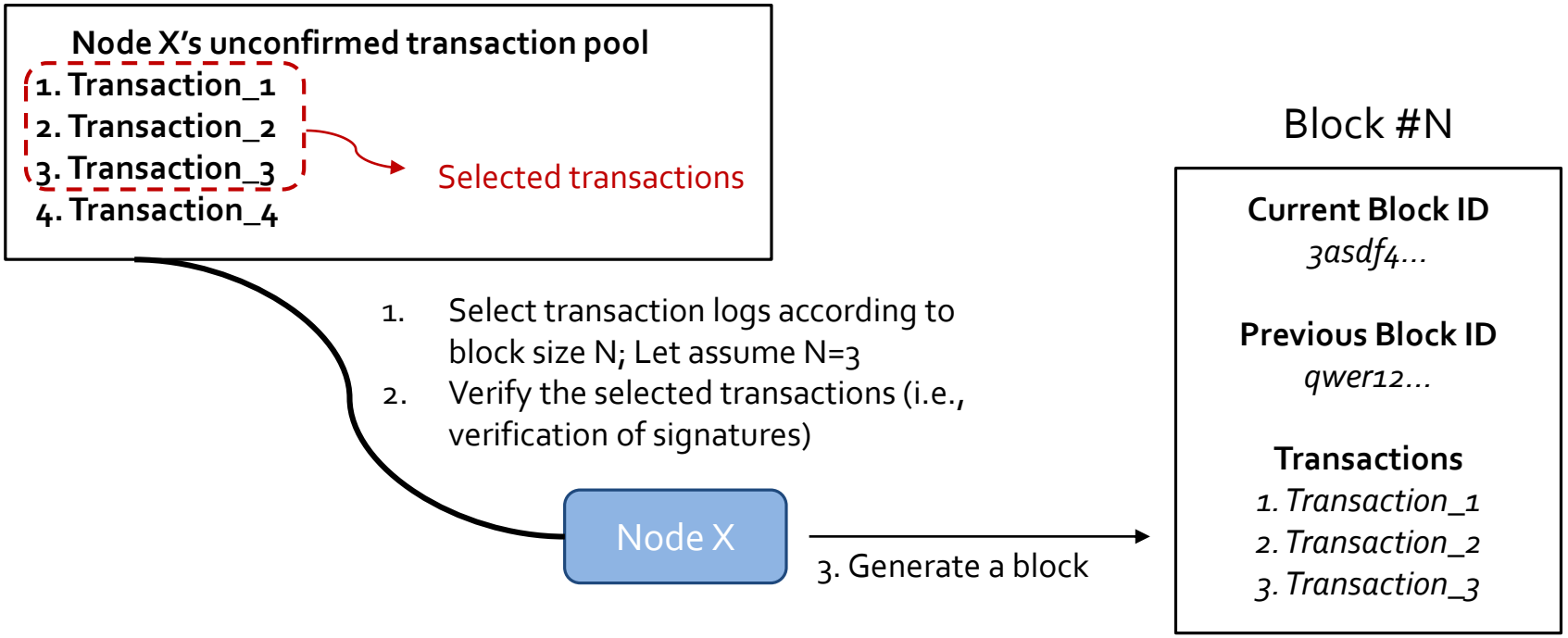
4. Node Y shares the transaction data from Alice



* $Trans_{ID}$: Transaction data from an entity with ID, $Priv_{ID}$: The private key of an entity with ID
$Sign_{priv_{ID}}()$: A digital signature algorithm (e.g., ECDSA) with a private key ($priv_{ID}$)
σ_{ID}: A digital signature value of an entity with ID

Blockchain Details

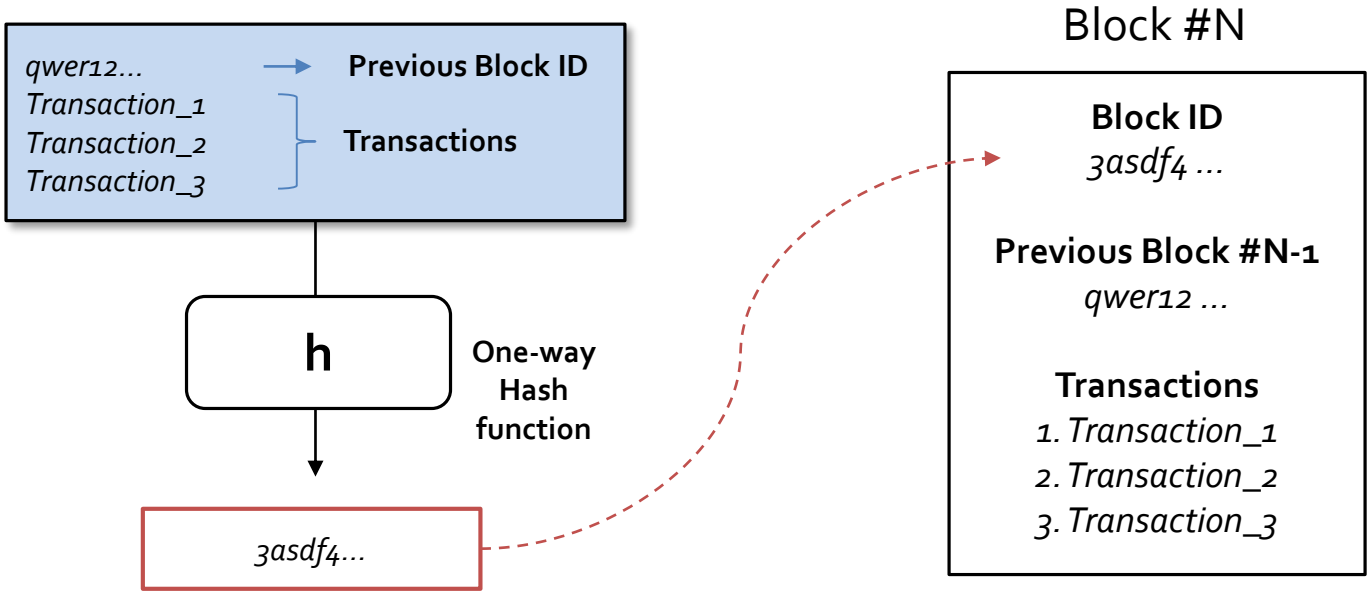
- 블록 생성 (Block generation)
  - 블록체인에 연결된 노드들이 자발적으로 블록을 생성
    - 블록을 생성하게 될 경우, 보상을 받음



Block ID is generated by a cryptographic hash function

Blockchain Details

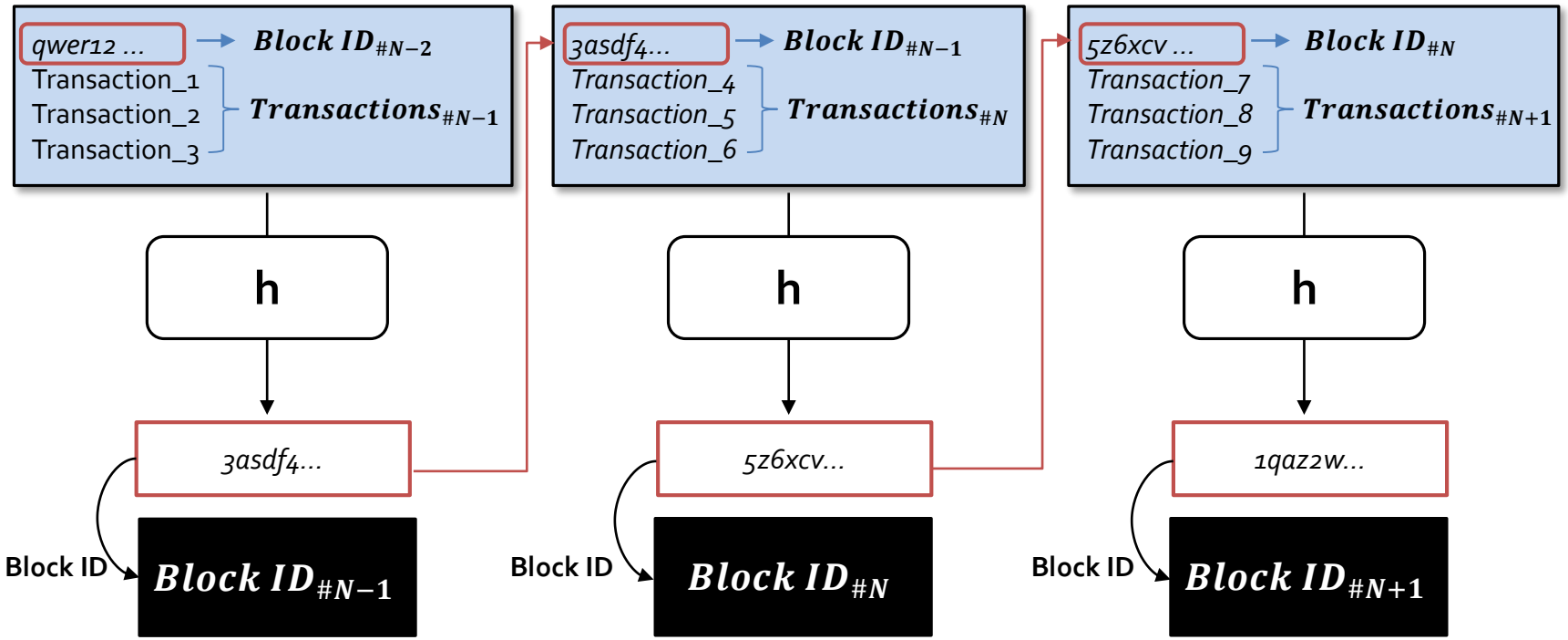
- 블록 생성 (Block generation)
  - Block ID에 대한 입력값은 이전의 Block ID와 트랜잭션 관련 값으로 구성됨



Block ID is generated by a cryptographic hash function

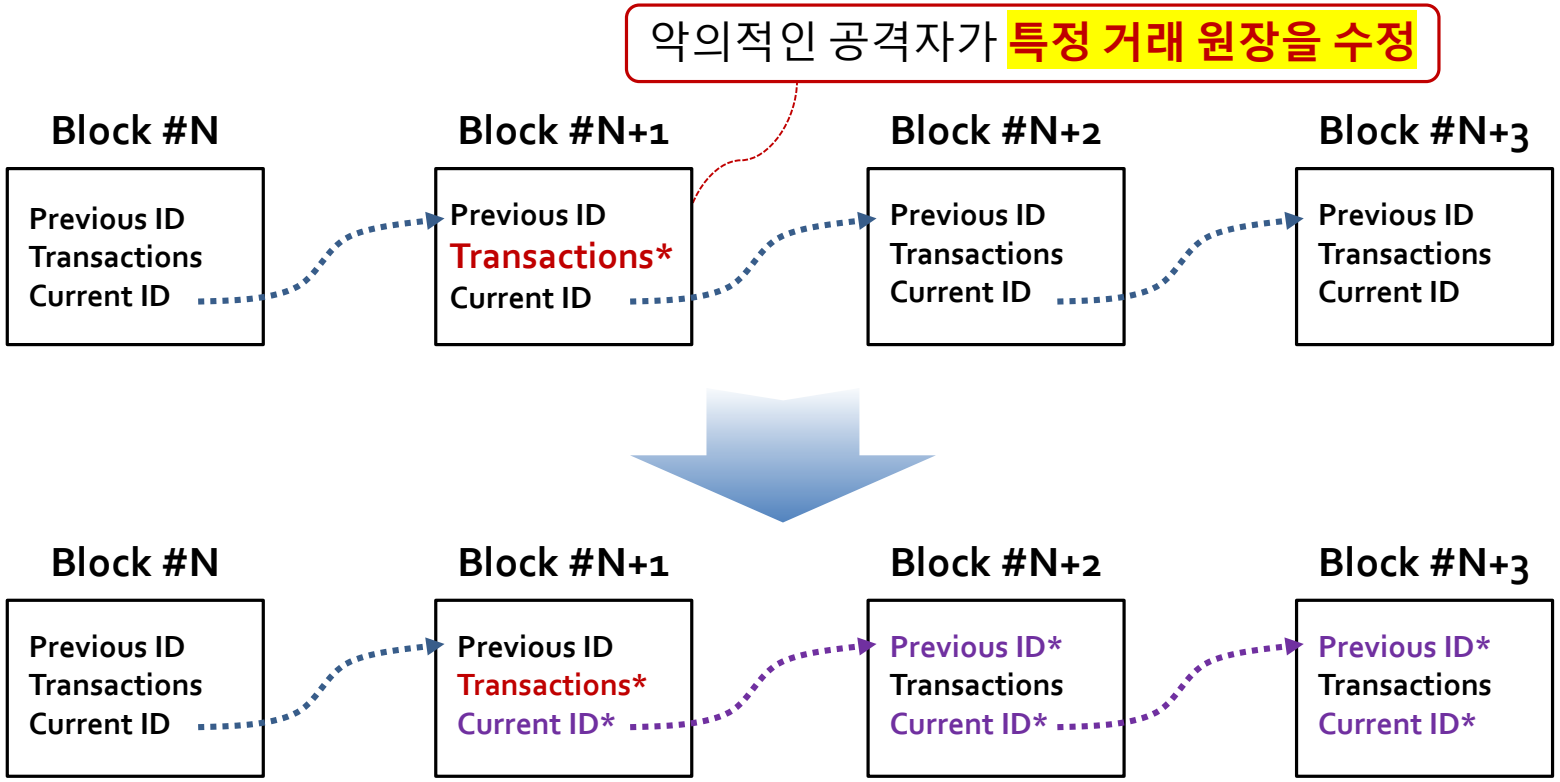
Blockchain Details

- 블록 생성 (Block generation)
  - 모든 블록들이 hash-chain의 방식으로 연결됨
    - 현재 블록에 이전 블록에 대한 ID가 hash값으로 구성됨
      - 지금까지의 모든 거래들에 대한 추적이 가능



Blockchain Details

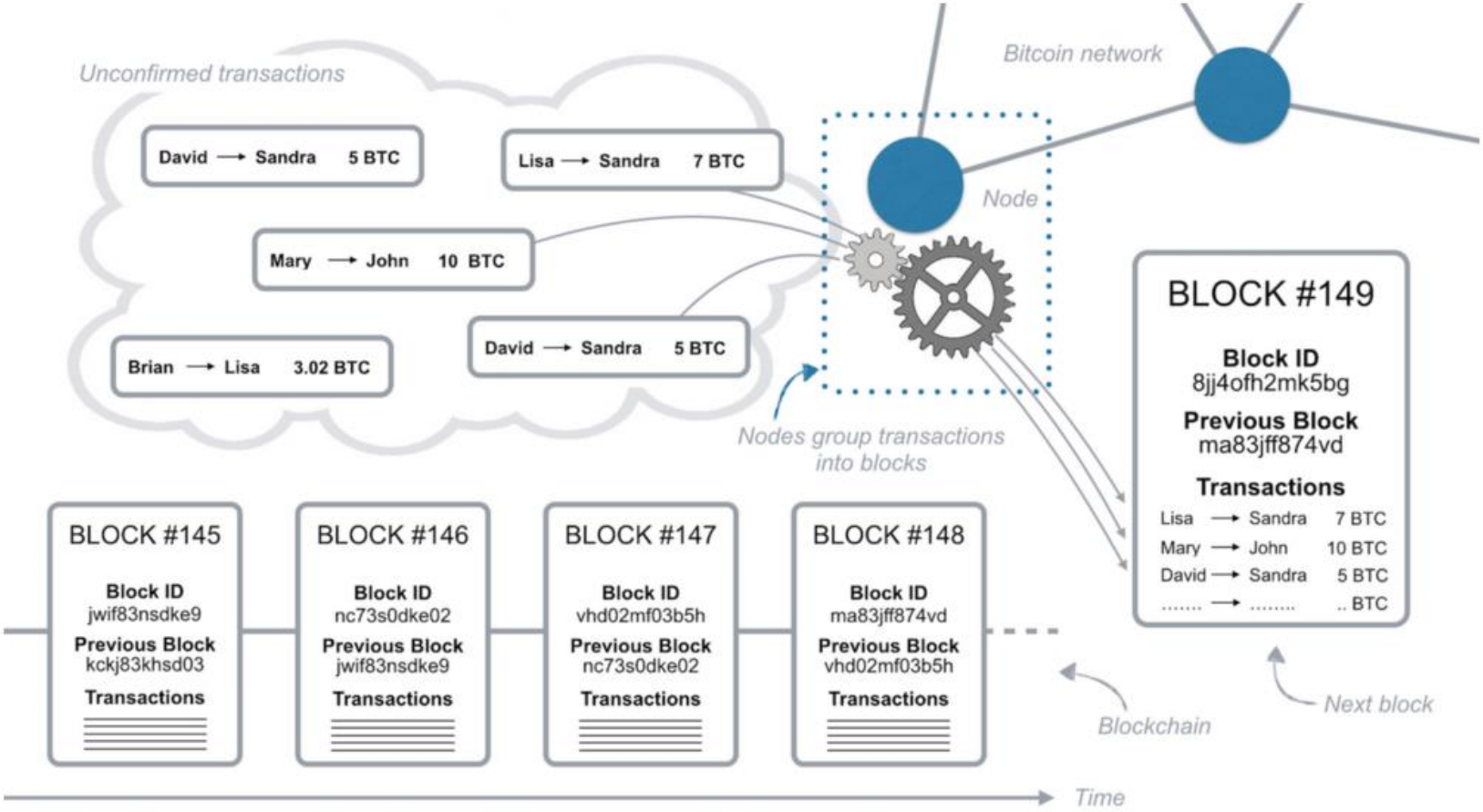
- 블록 연결 (Chaining blocks) - Data integrity



  - 블록체인에서 각 블록들이 이전 블록과 연결됨에 따라, 모든 블록들의 hash값에 영향을 줌
    - 이미 생성된 블록에 대해서 수정을 하게 될 경우, 새롭게 구성된 블록들에 대해서 기존 블록들과 비교가 가능

Blockchain Details

- 블록체인 예제: 비트코인 시스템



(Source: https://medium.com/@micheledaliessi/how-does-the-blockchain-work-98c8cd01d2ae)

Blockchain Details

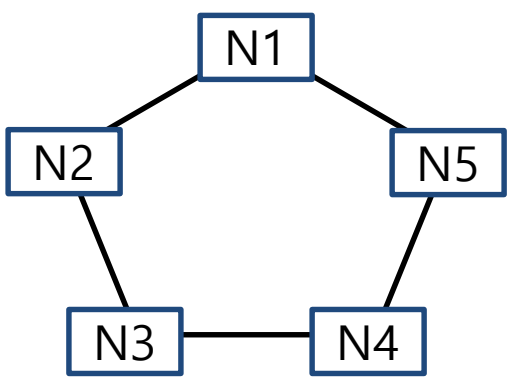
- Openness of blockchain
  - 개방형 블록체인 (Public / Permissionless blockchain,)
    - 네트워크에 참여하고 싶은 만큼 노드를 참여함
    - 악의적인 공격자로부터 보호 및 접근에 대한 제어가 필요하지 않음
    - 노드를 운용하는 사용자(채굴자)에게 보상으로 암호화폐 송금
      - Bitcoin, Ethereum, …
  - 허가형 블록체인 (Private / Permissioned blockchain)
    - 허가된 노드만이 해당 블록체인에 참여 가능 (참여자 제한)
      - '참여 노드 수'를 항상 파악
      - 노드들의 블록 생성 및 블록 관리를 통제
    - 노드 운영자에게 보상이나 트랜잭션 수수료를 줄 필요 없음
      - Hyperledger fabric, Quorum, Digital Asset Holdings…

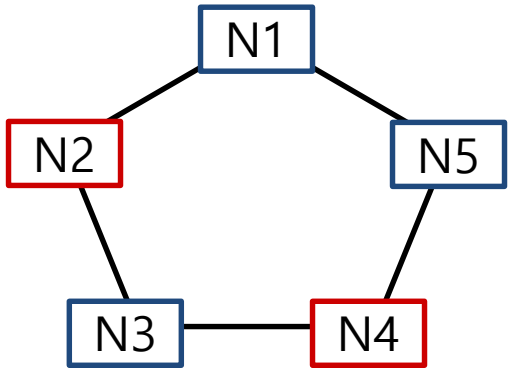
Blockchain Details

Openness of blockchain

Validator node
(Can both initiate/receive and validate transactions)

Member node
(Can only initiate/receive transactions)



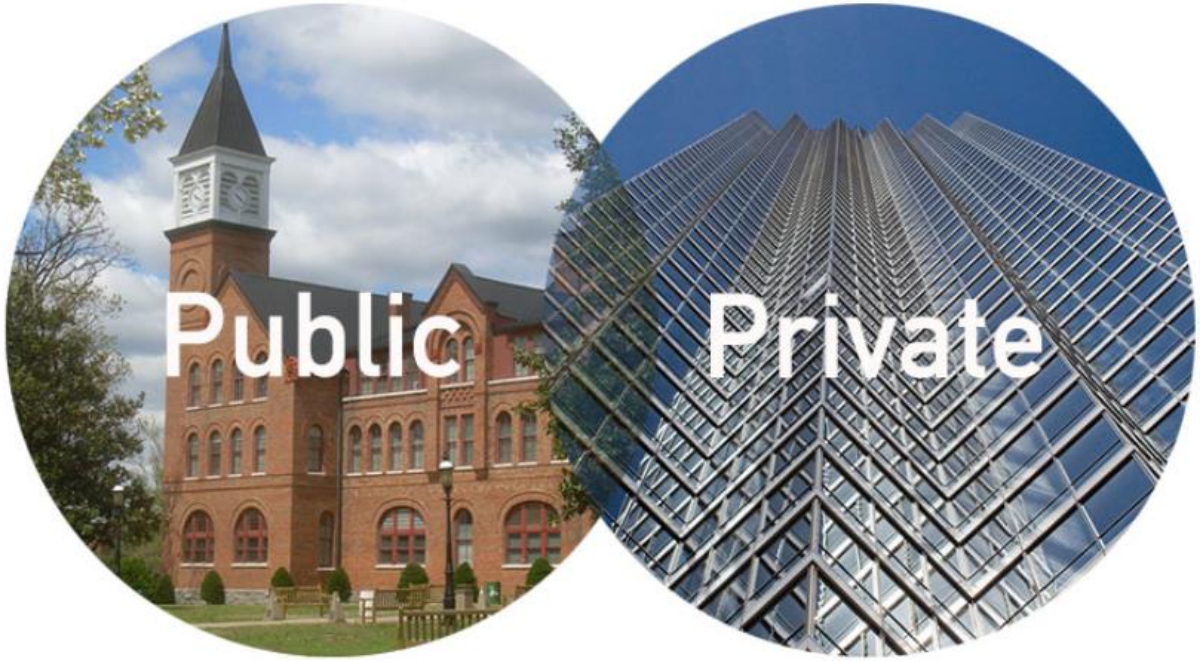


	Permissionless (public)	Permissioned (private)
How do you get access to blockchain networks?	**Open access**	Open access or **Authorized access**
Who are the block generator?	**Anyone** (fully decentralized block generators)	**Pre-selected**, **semi-trusted block generators**
What can it be used for?	Open access applications	Enterprise-level systems

(Sources: Blockchain, smart contracts and use cases for the Legal Hackers, 2017)

Blockchain Details

- Openness of blockchain
  - Data access
  - Consensus
    - Permissioned or Permissionless



[Source: https://allianceforscience.cornell.edu/blog/2015/09/celebrating-the-public-private-partnership-in-agriculture/]

Blockchain Details

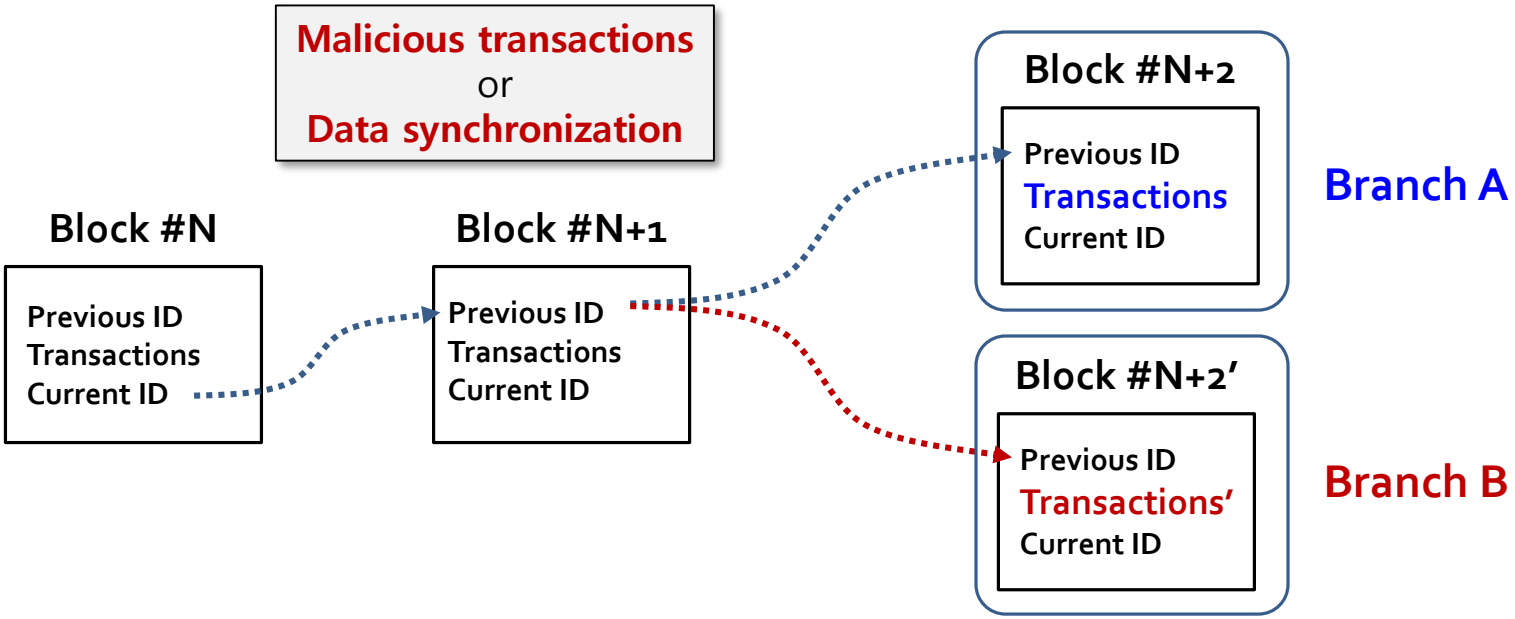
- 합의 (Consensus)
  - 노드들간의 동의를 의미
    - 즉, 기존의 블록체인 네트워크가 구성되어 있고, 다수의 블록들이 연결되어 있을 때, 새로운 블록을 체인에 연결해야 하는지에 대한 동의 과정을 의미
    - P2P 네트워크에서 통신 지연 및 정보의 전송 속도차에 의해, 데이터를 변조 및 위조하려는 공격 의도가 없더라도 정확한 정보를 각 피어 노드들에게 공유하기 어려움
    - 블록체인 네트워크에서 각 노드간 중요 정보 도달에 대한 시간 차이가 있더라도, 새롭게 생성된 블록에 대한 정당성을 검토하여 동의를 얻기 위한 알고리즘

Blockchain Details

- 합의 (Consensus)
  - 블록체인 포크 (Fork of blockchain)
    - 유효하지 않은 블록 생성
    - 데이터 동기화
  - 합의 알고리즘
    - Proof of Work (PoW) - Bitcoin, Ethereum
    - Proof of Stake (PoS) - Ethereum
    - Byzantine Fault Tolerance (BFT) - Hyperledger fabric
    - Federated Byzantine Agreement (FBA) - Stellar
    - Proof of Elapsed Time (PoET) - Intel-SGX based

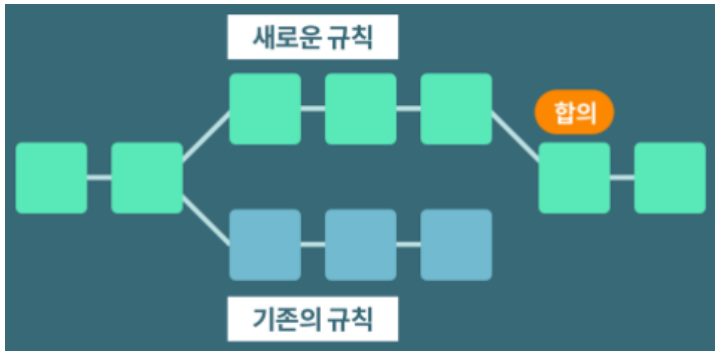
Blockchain Details

- 합의 (Consensus)
  - 블록체인 포크 (Fork of blockchain)
    - **악의적인 트랜잭션 발생** 또는 **데이터 동기화 이슈**가 있을 경우, 블록체인은 일시적으로 포크 수행



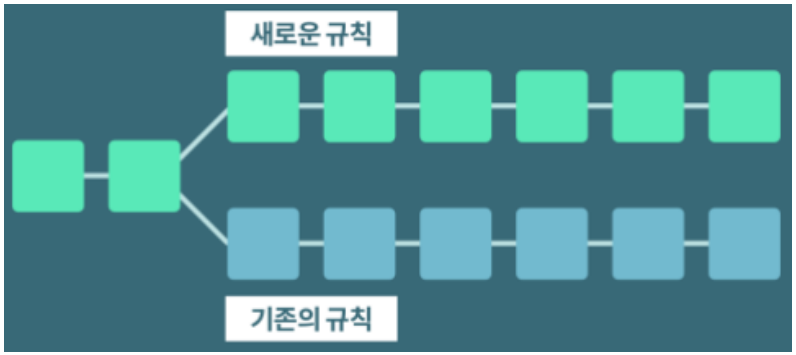
Blockchain Details

- 합의 (Consensus)
  - 블록체인 포크 (Fork of blockchain)



소프트 포크 (Soft Fork)

- Tightening the rules (e.g., 1MB -> 0.5MB)
- Backwards compatible (이전 버전과 호환 가능)
  - Old nodes accept new blocks



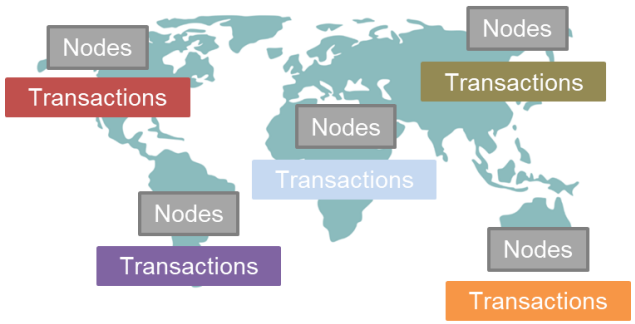
하드 포크 (Hard Fork)

- Expanding the rules (e.g., 1MB -> 8MB)
  - Bitcoin Cash (BCH)
- Not backwards compatible (이전 버전과 호환 가능)
  - Old nodes don't accept new blocks

[Source: 쉽게 설명하는 블록체인 : 블록체인의 허점과 하드포크, 소프트포크 | 뱅크샐러드 (banksalad.com)

Blockchain Details

- 합의 (Consensus)
  - 블록체인 포크 (Fork of blockchain)
    - 손상된 블록체인 클라이언트/노드들의 **잘못된 트랜잭션/블록 생성** 또는 블록체인 노드 간의 **동기화 이슈**로 인해 발생
    - 유효하지 않은 블록 / 트랜잭션
      - E.g, 이중 지불 문제
        - A가 5 BTC를 가지고 있는데, 5BTC를 B와 C에게 동시에 전송
    - 데이터 동기화
      - 분산 네트워크에서 통신 지연 및 정보의 전송 속도차에 의해, 각 노드들은 동일한 정보를 가지고 있지 않을 수 있음



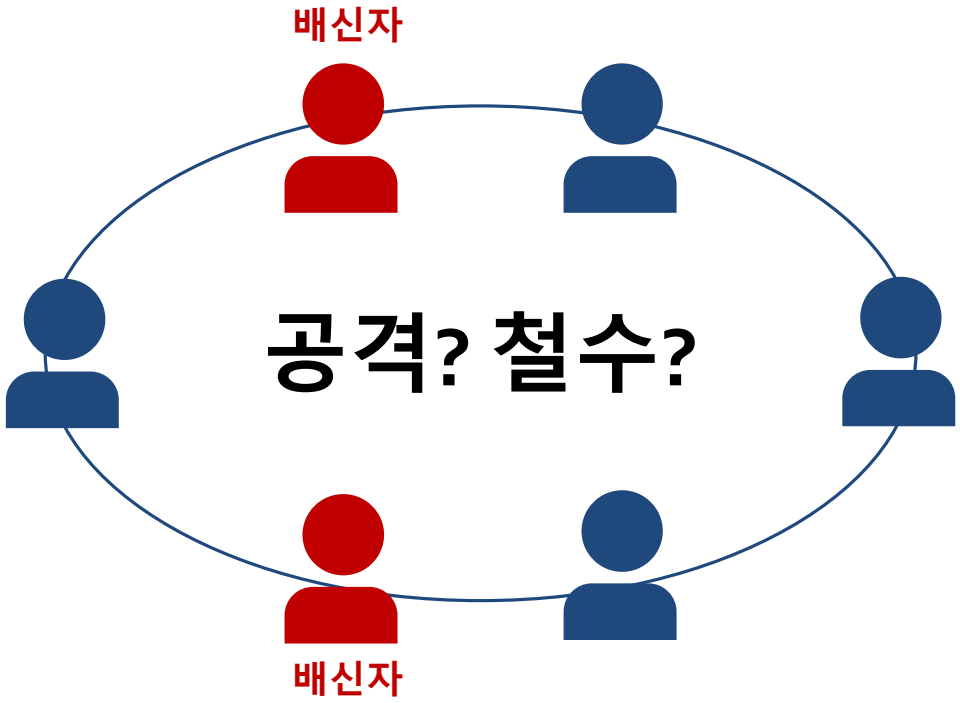
Blockchain Details

- 합의 (Consensus)
  - 블록체인 포크 (Fork of blockchain)

잘못된 트랜잭션 / 블록은 비잔틴 장군 문제 (Byzantine Generals Problem)과 관련됨

Blockchain Details

- 합의 (Consensus)
  - 블록체인 포크 (Fork of blockchain)
    - 비잔틴 장군 문제 (**B**yzantine **G**enerals **P**roblem)

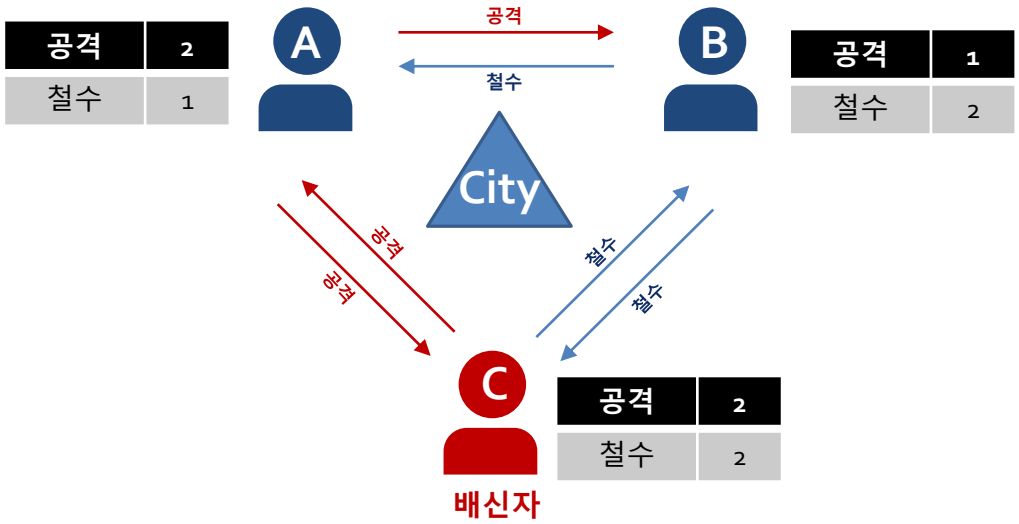


n명의 장군이 공격할지 철수할지 합의

n명의 장군 중 최대 f명의 **배신자**가 존재

Blockchain Details

- 합의 (Consensus)
  - 블록체인 포크 (Fork of blockchain)
    - 비잔틴 장군 문제 (**B**yzantine **G**enerals **P**roblem)



- 다수결의 원칙으로 장군들의 행동을 결정하게 될 경우
  - A와 B는 다르게 행동 (A는 공격, B는 철수, C는 행동 X)
  - 모두가 동일한 결과를 내야 하는 상황에서, 문제가 발생함

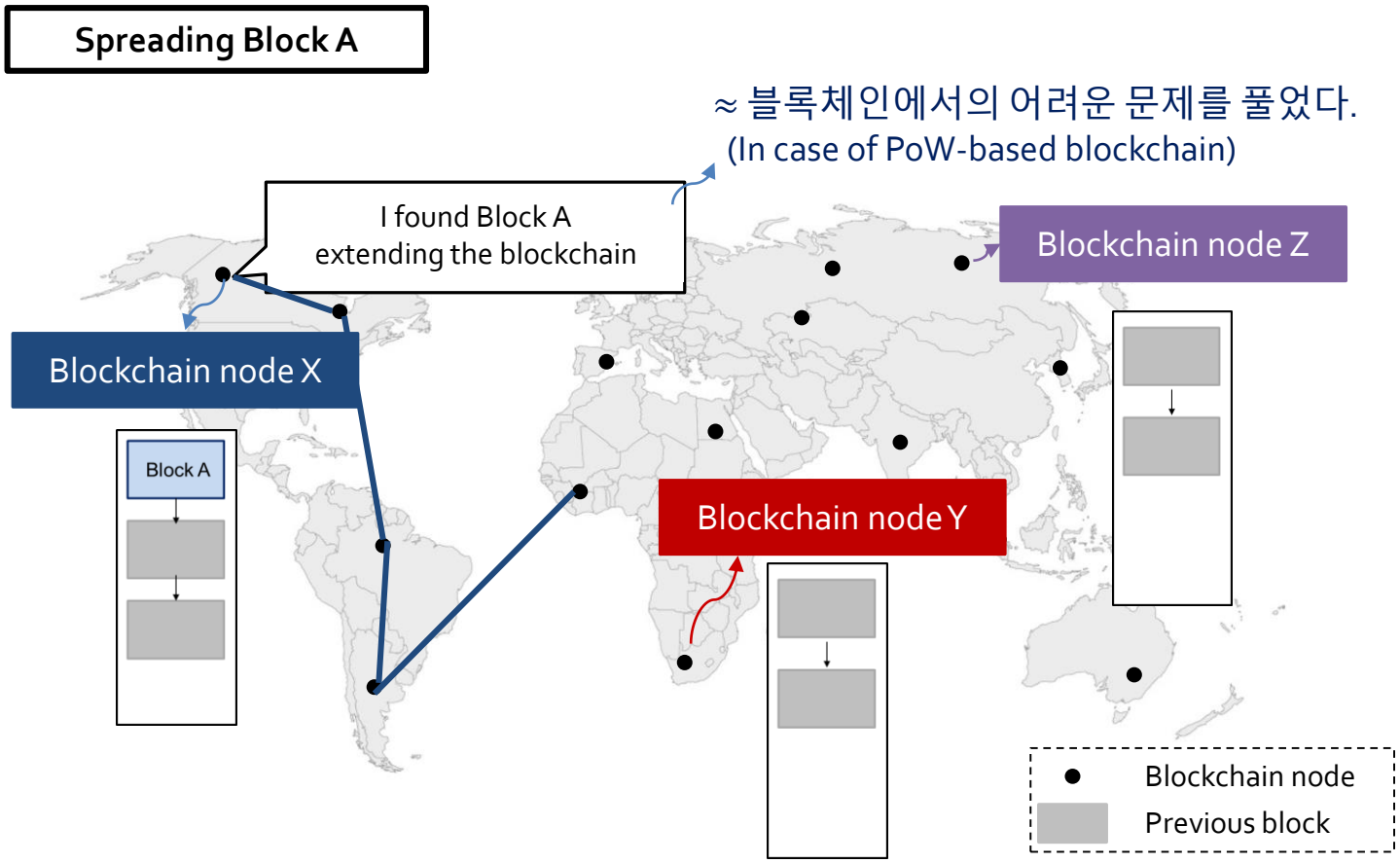
Blockchain Details

- 합의 (Consensus)
  - 블록체인 포크 (Fork of blockchain)
    - 블록체인 시스템에서의 BGP

BGP		Blockchain
Agree on a strategy	Objective	Agree on valid transactions
Separated camp	Spatial Distribution	Distributed nodes in the blockchain network
Loyal troop and loyal generals	The Good Ones	Truthful nodes
Traitors	The Bad Ones	Evil nodes
Corrupt a message	The Attack	Add an invalid transaction to the blockchain
How to know which message is true	The Problem	How to know which transaction is valid

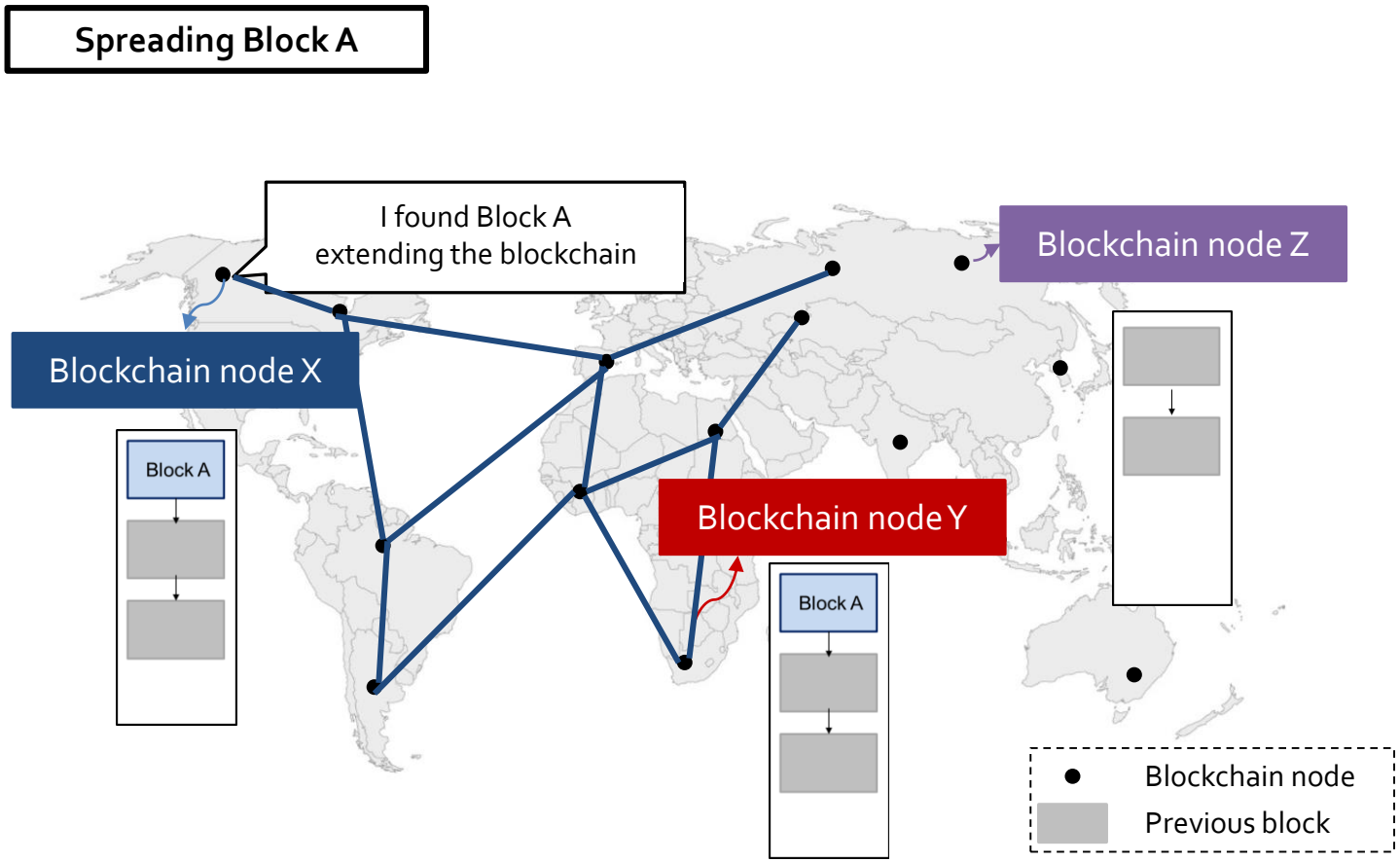
Blockchain Details

- 합의 (Consensus)
  - 블록체인 포크 (Fork of blockchain)
    - 데이터 동기화



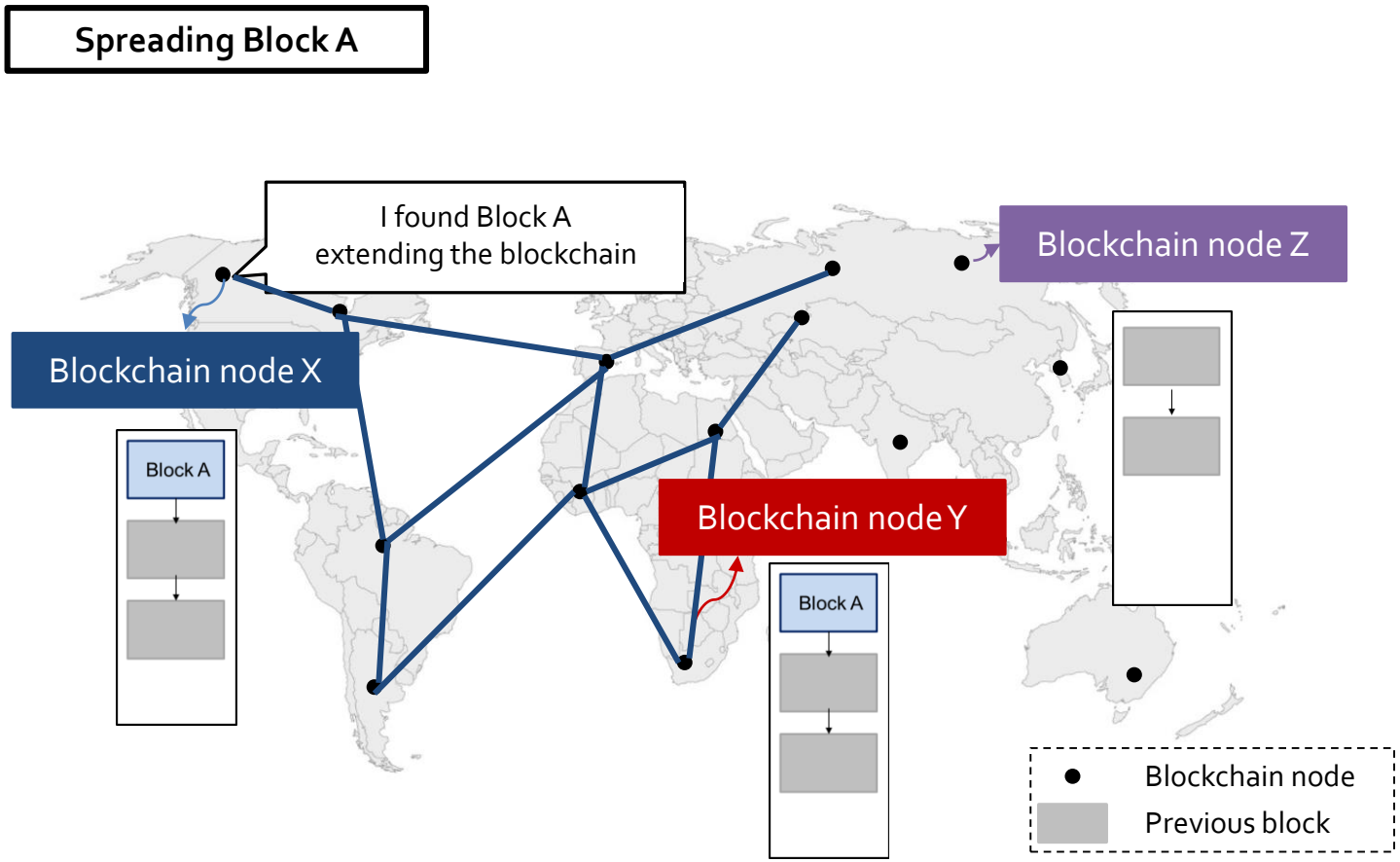
Blockchain Details

- 합의 (Consensus)
  - 블록체인 포크 (Fork of blockchain)
    - 데이터 동기화



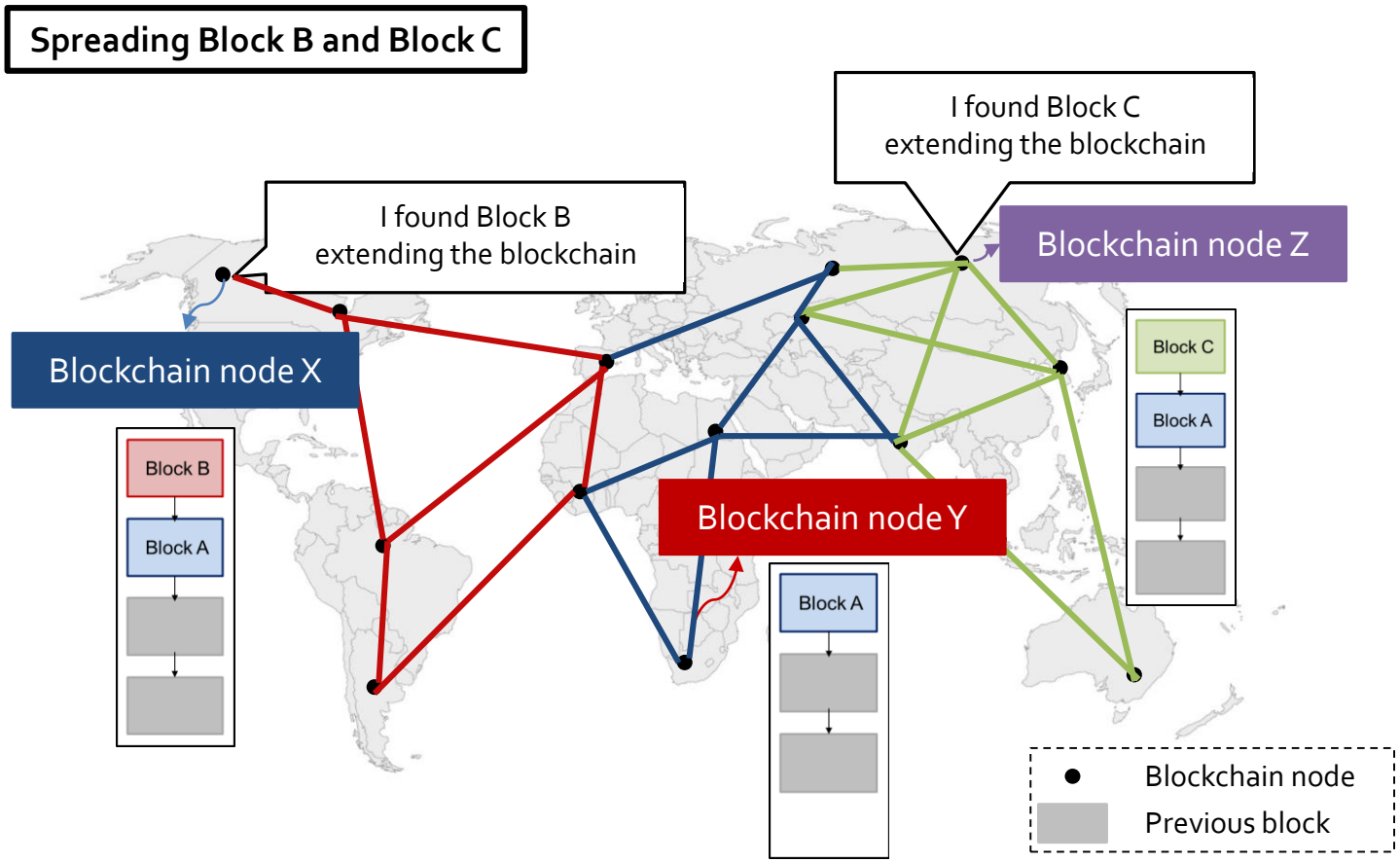
Blockchain Details

- 합의 (Consensus)
  - 블록체인 포크 (Fork of blockchain)
    - 데이터 동기화



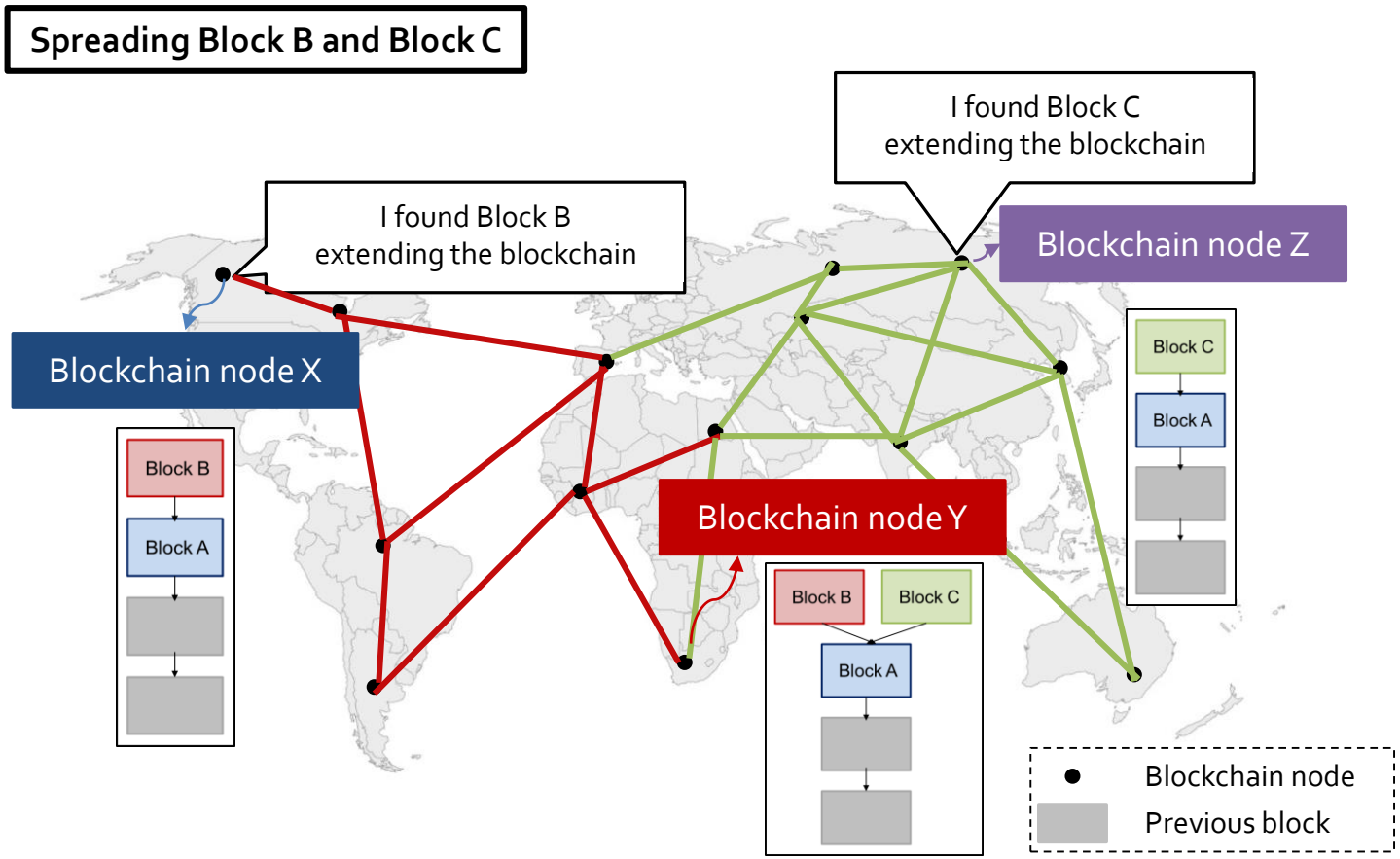
Blockchain Details

- 합의 (Consensus)
  - 블록체인 포크 (Fork of blockchain)
    - 데이터 동기화



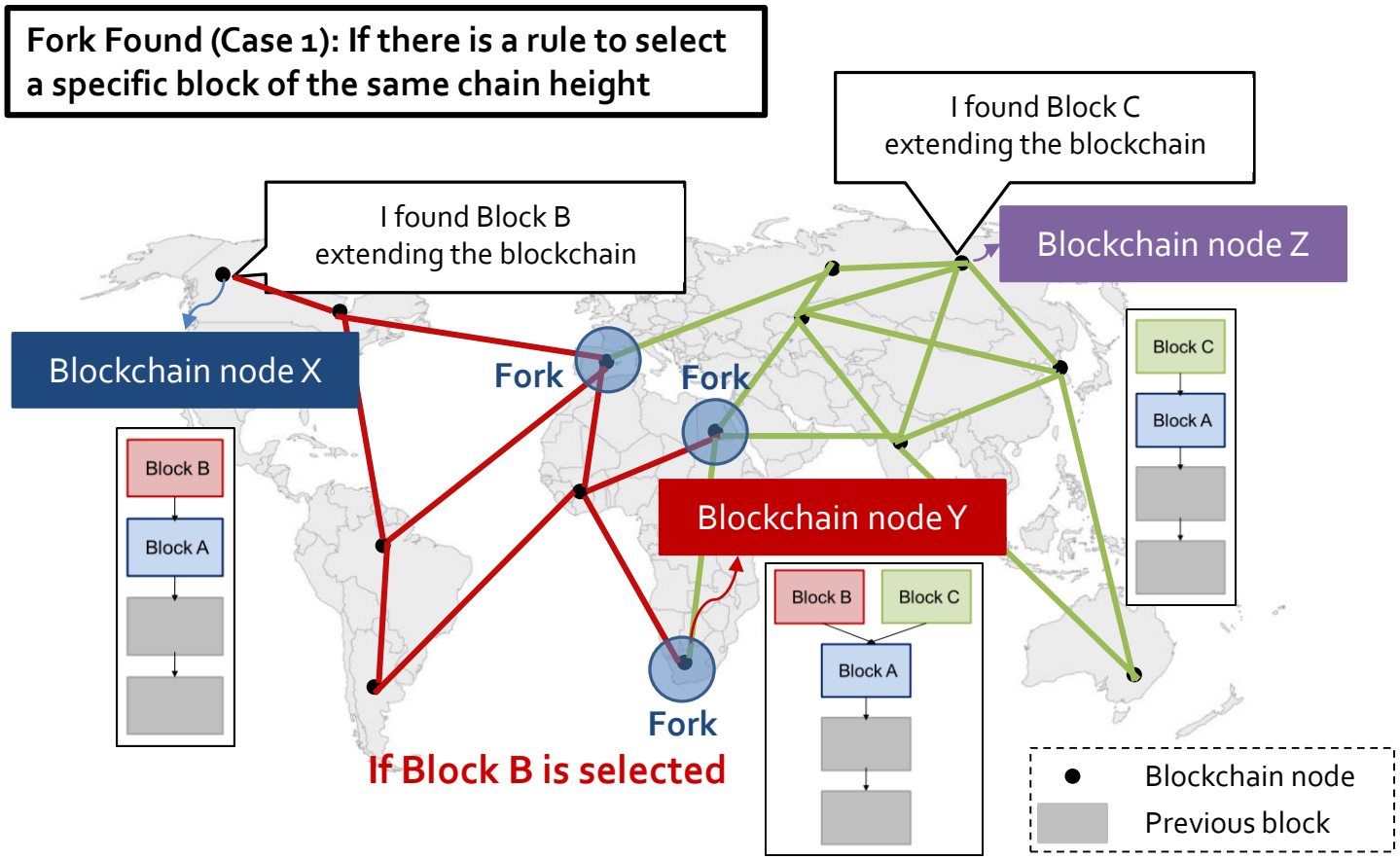
Blockchain Details

- 합의 (Consensus)
  - 블록체인 포크 (Fork of blockchain)
    - 데이터 동기화



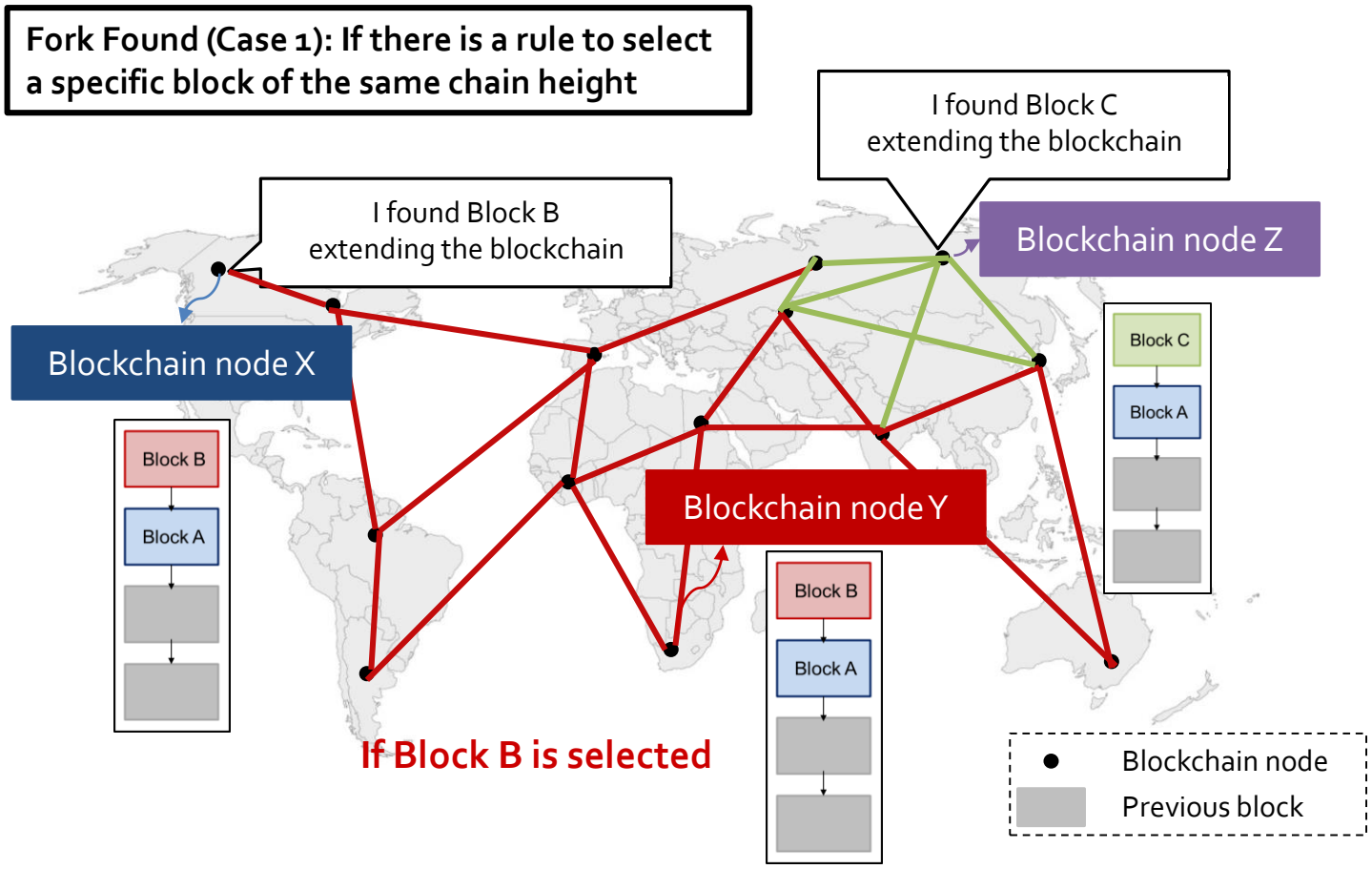
Blockchain Details

- 합의 (Consensus)
  - 블록체인 포크 (Fork of blockchain)
    - 데이터 동기화



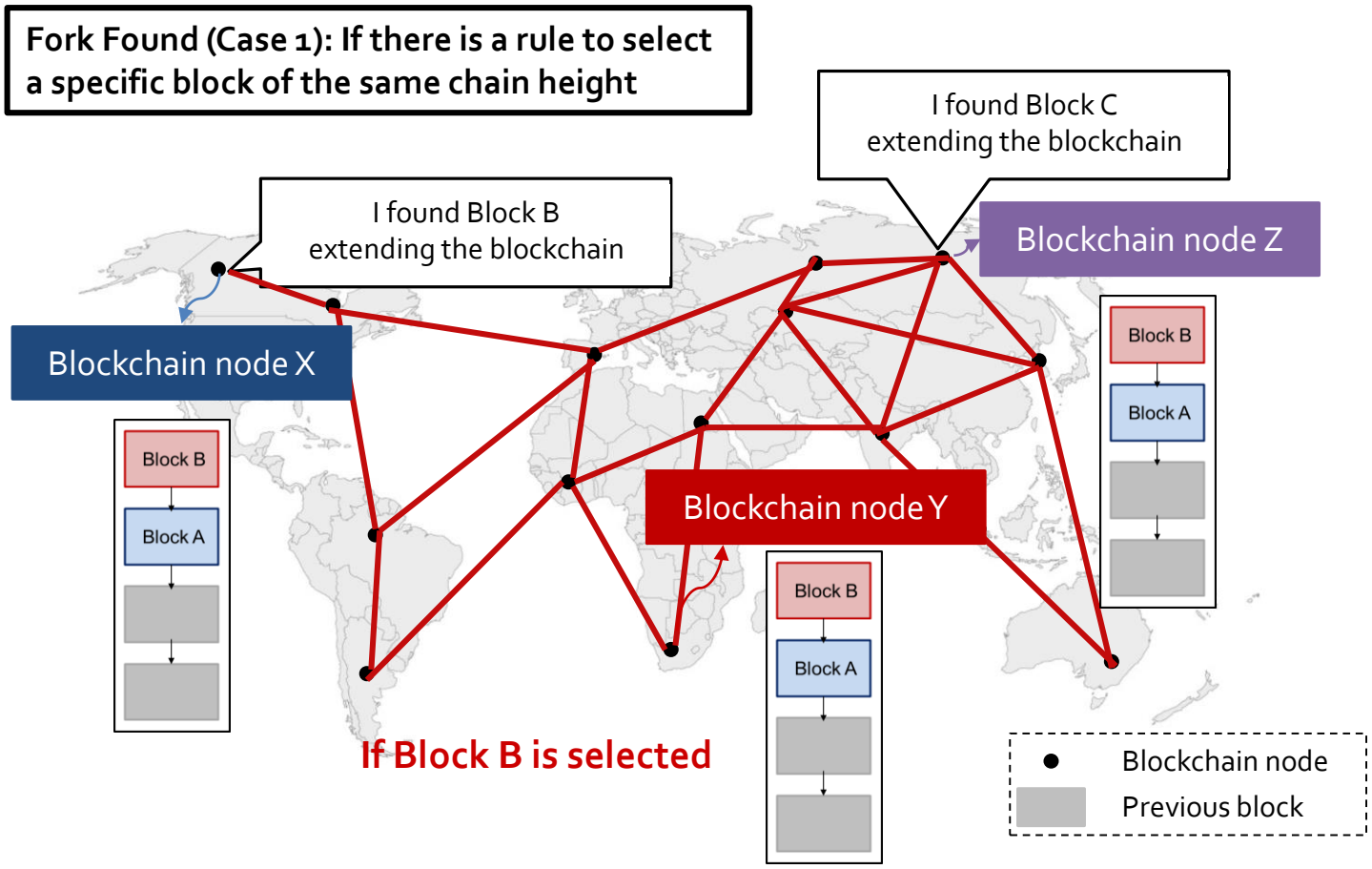
Blockchain Details

- 합의 (Consensus)
  - 블록체인 포크 (Fork of blockchain)
    - 데이터 동기화



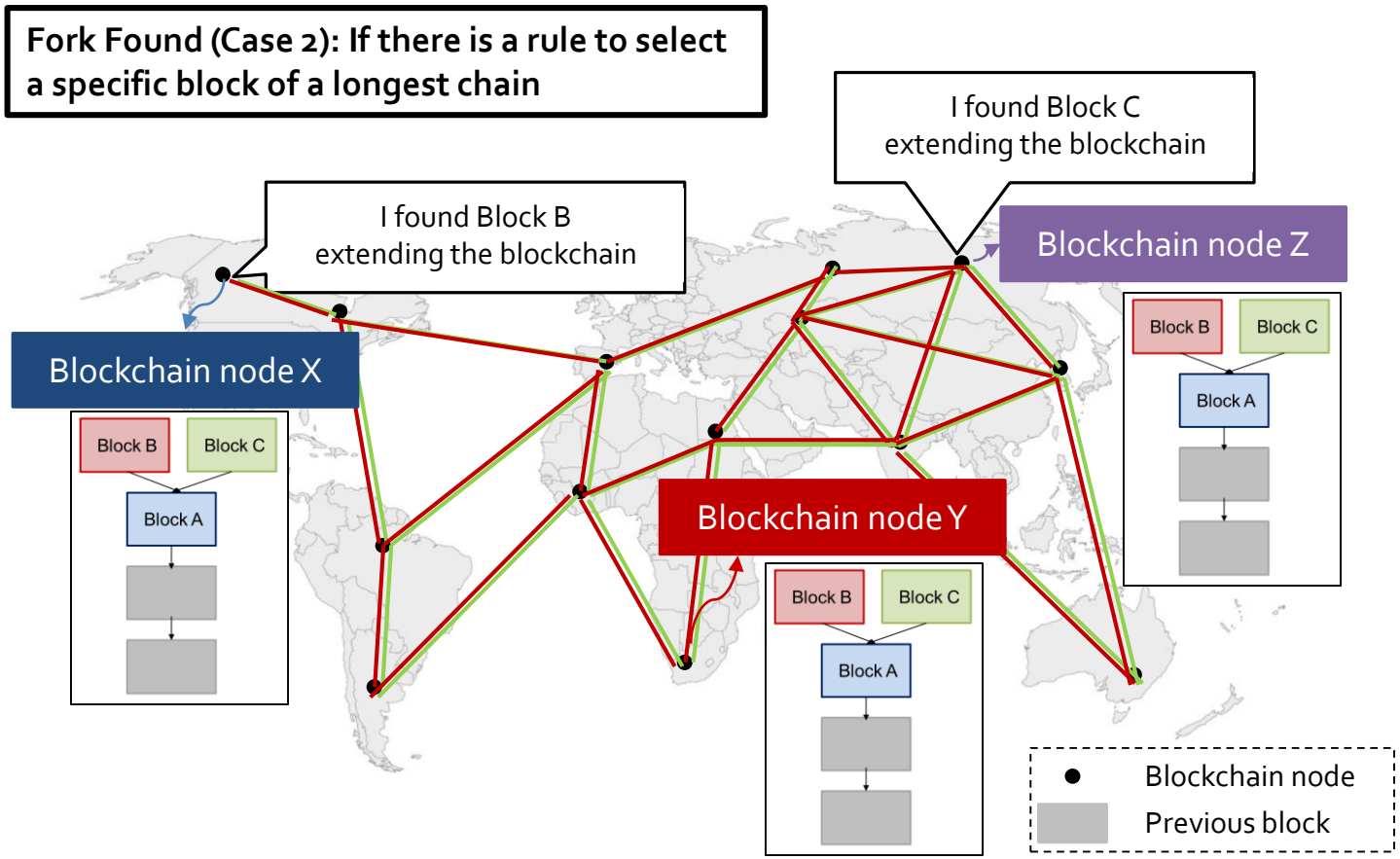
Blockchain Details

- 합의 (Consensus)
  - 블록체인 포크 (Fork of blockchain)
    - 데이터 동기화



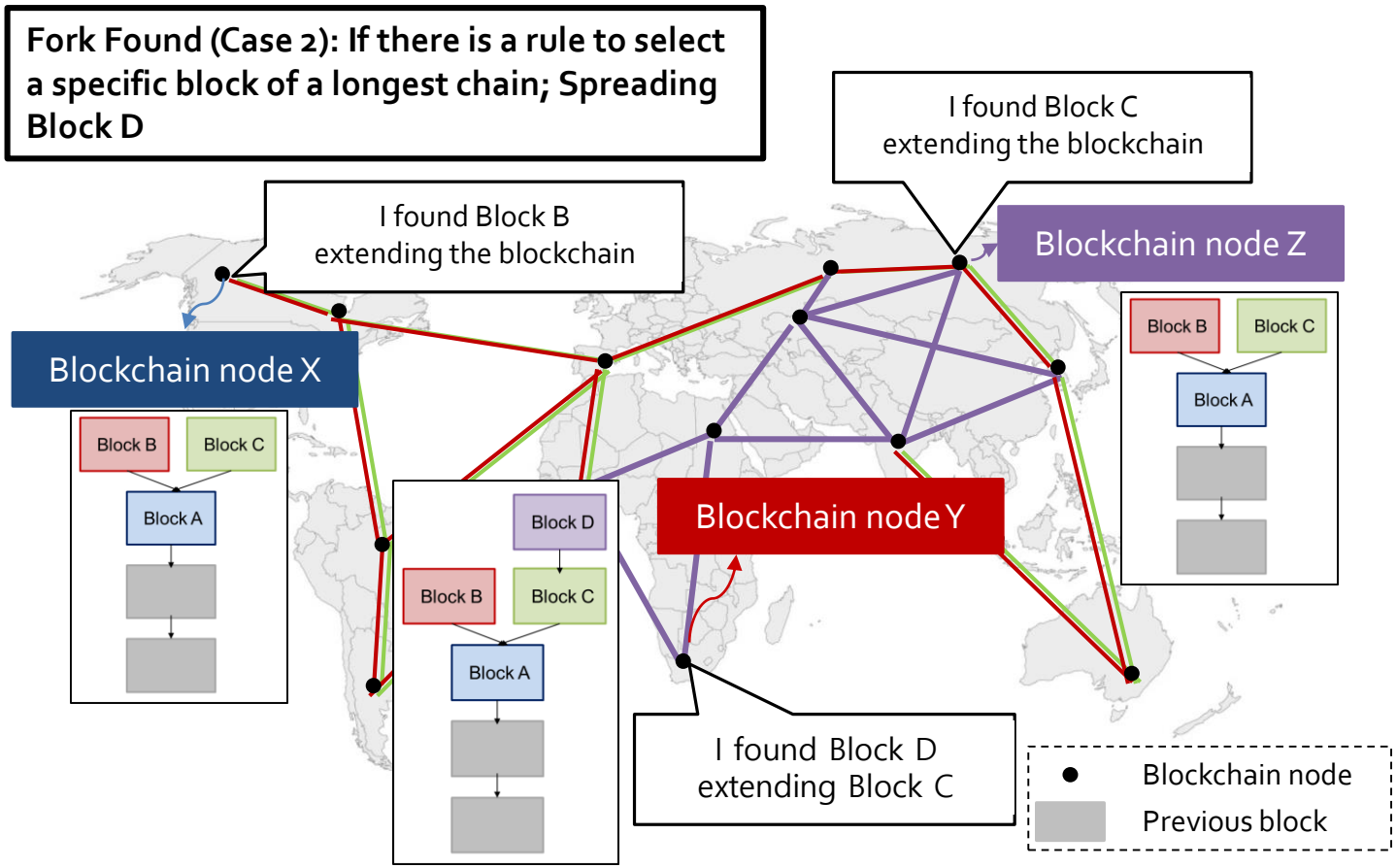
Blockchain Details

- 합의 (Consensus)
  - 블록체인 포크 (Fork of blockchain)
    - 데이터 동기화



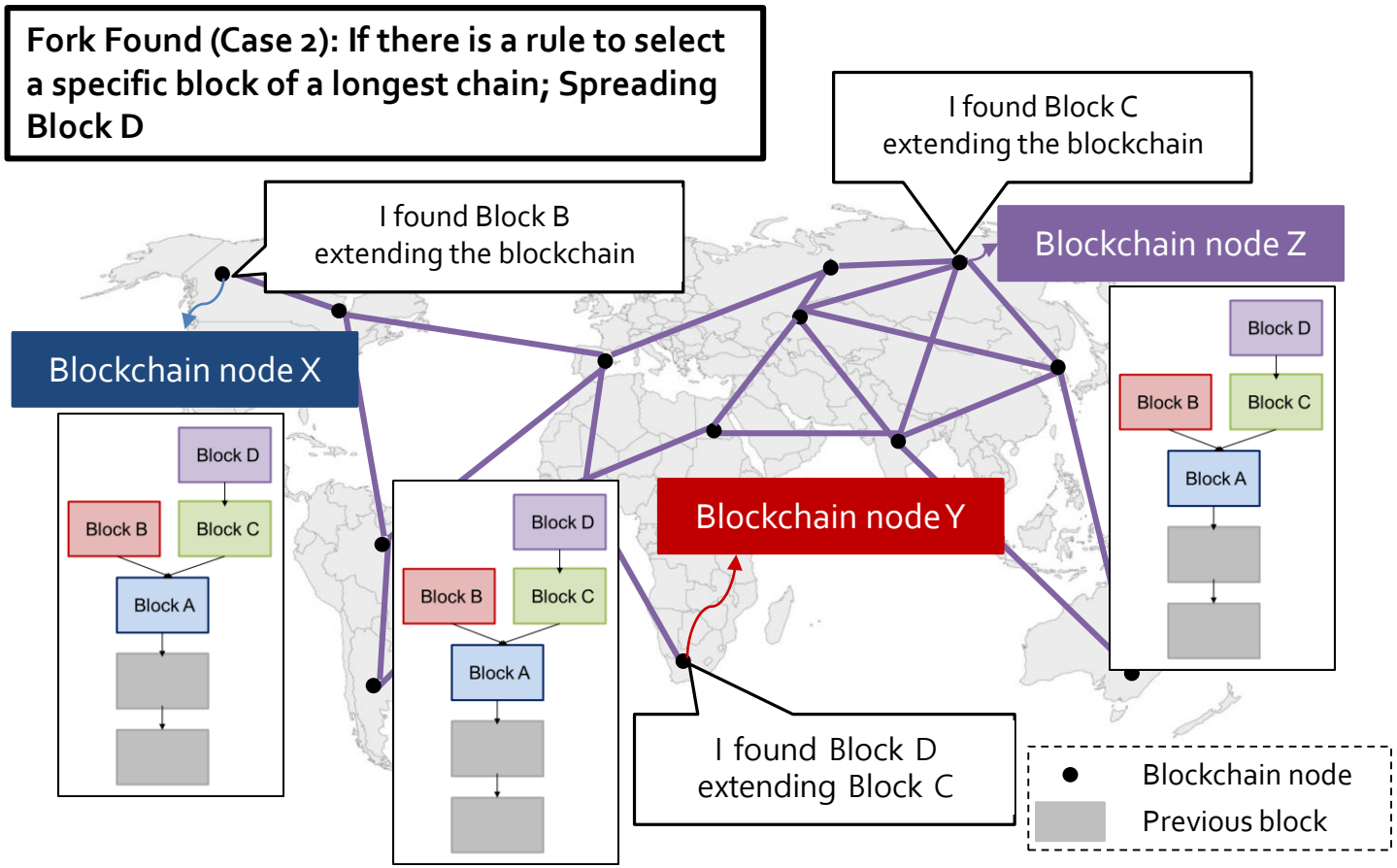
Blockchain Details

- 합의 (Consensus)
  - 블록체인 포크 (Fork of blockchain)
    - 데이터 동기화



Blockchain Details

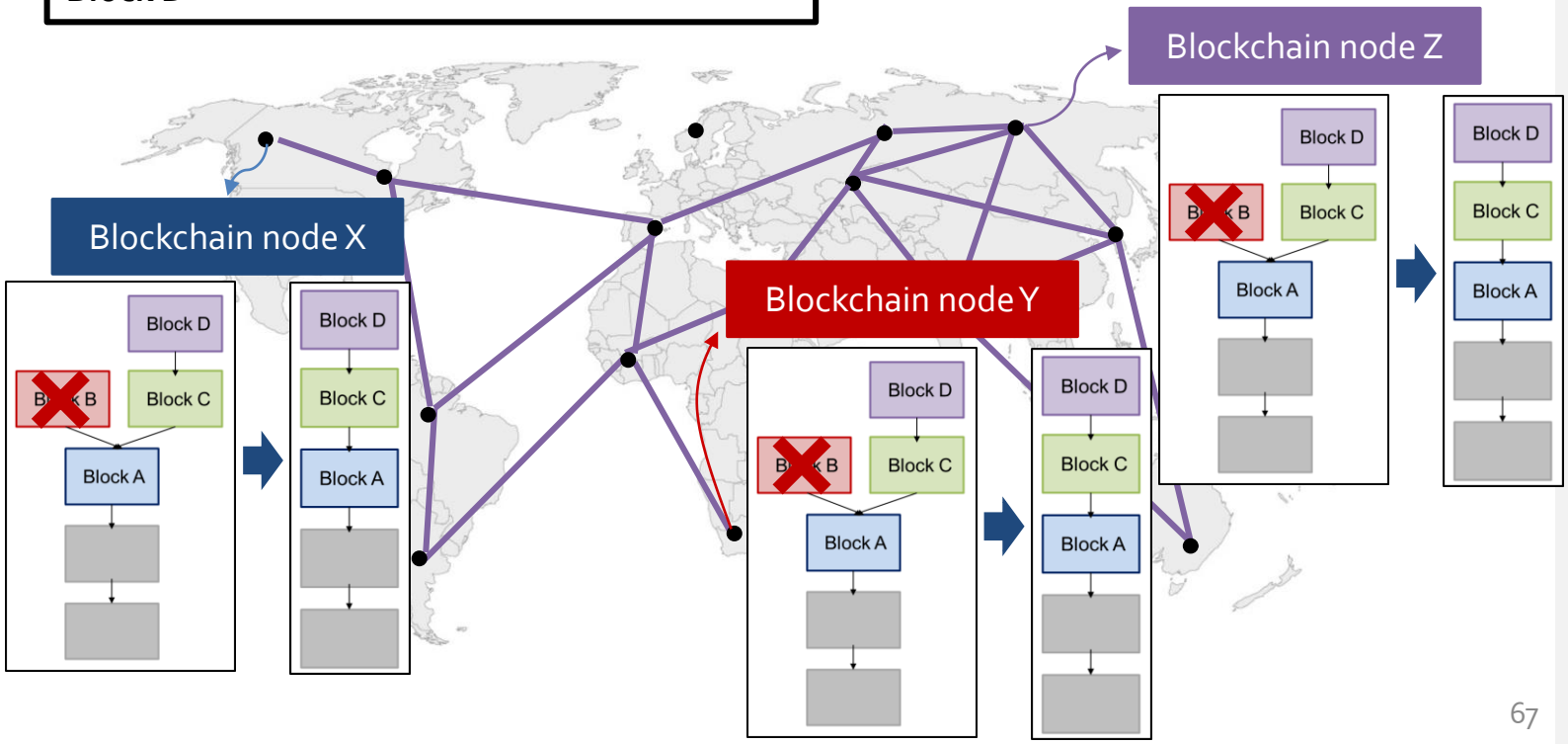
- 합의 (Consensus)
  - 블록체인 포크 (Fork of blockchain)
    - 데이터 동기화



Blockchain Details

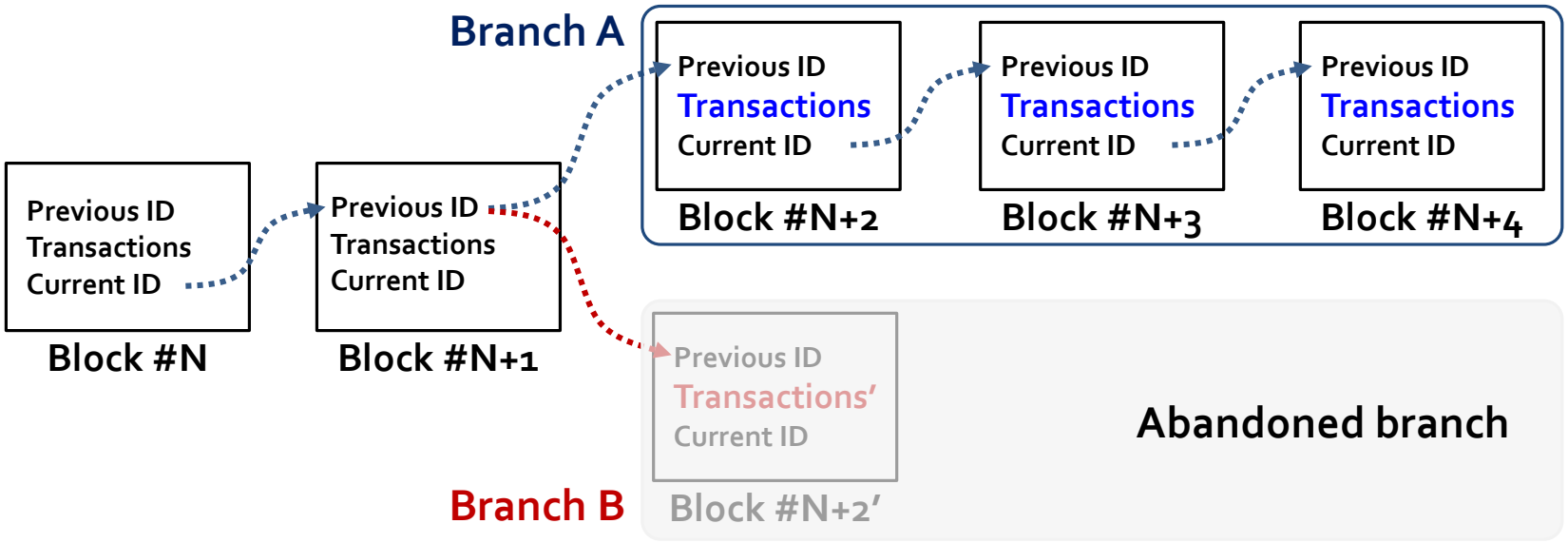
- 합의 (Consensus)
  - 블록체인 포크 (Fork of blockchain)
    - 데이터 동기화

Fork Found (Case 2): If there is a rule to select a specific block of a longest chain; Spreading Block D



Blockchain Details

- 합의 (Consensus)
  - 블록체인 포크 (Fork of blockchain)
    - 두 개 이상의 블록 체인 분기(Fork)가 일어났을 경우
      - 블록체인 시스템은 신뢰할 수 있는 중앙 컨트롤 시스템이 없기 때문에, 합의 알고리즘을 통해 특정 분기를 구성하는 블록들을 선택함



Blockchain Details

- 합의 (Consensus)
  - 블록체인 합의 모델은 블록체인에 연결된 모든 노드들이 동일한 데이터를 동기화한 상태로 유지를 목표
  - 합의를 달성하기 위해서는 일부 노드가 실패하거나 네트워크에 대한 공격을 통해 일부 노드를 신뢰할 수 없는 상황일 경우에도 모든 트랜잭션에 대해 만장일치가 요구됨
  - 블록체인의 시스템에 따라 합의 알고리즘의 방식이 다르게 설정됨

Blockchain Details

- 합의 (Consensus)
  - 작업증명 (Proof-of-Work)
    - 새로운 블록을 생성하기 위해 각 블록체인의 노드들이 특정 퍼즐 문제를 푸는 작업 (암호화폐 채굴) 을 수행함
  - 지분증명 (Proof-of-Stake)
    - 새로운 블록을 생성하기 위해 지분 증명은 채굴 작업을 블록체인 시스템에서 사용자의 지분 또는 암호 화폐의 소유권과 관련된 접근 방식으로 대체
  - Byzantine Fault Tolerance (BFT)
    - 새로운 블록체인의 노드를 추가하기 위해, 다른 노드들의 승인이 필요

Blockchain Details

- 합의 (Consensus)
  - Federated Byzantine Agreement (FBA)
    - 모든 블록체인 노드들은 신뢰할 수 있는 그룹을 형성하고, 신뢰할 수 잇는 그룹의 블록체인에서 합의 과정을 수행
  - 경과시간증명 (Proof of Elapsed Time)
    - 모든 블록체인 노드들은 Intel SGX와 같은 TEE (Trusted Execution Environments)를 실행
    - PoET는 TEE에 의해 보호되는 랜덤 리더 선출 모델 (random leader election model) 또는 복권 (lottery based election model) 기반 선거 모델을 사용하고, 해당 리더 노드가 트랜잭션을 검증하여 새로운 블록을 생성함

Summary

- Cryptography
  - Cryptographic hash function and Digital signature
- Time synchronization on decentralized networks
  - With timestamp with a centralized server
  - With hash-chain in a decentralized setting
- Blockchain Details
  - Blockchain (Generation of transactions and blocks)
  - Openness (Public vs. private)
  - Consensus (Fork of blockchain and Consensus models)

Reference

- Lecture slides from BLOCKCHAIN @ BERKELEY

Q & A