알기 쉬운

정보보호개론 3판

흥미로운 암호 기술의 세계

INFORMATION SECURITY and CRYPTOGRAPHY

INFINITYBOOKS
인피니티북스

CHAPTER 16
암호 기술과 현실세계

Section 01
암호 기술의 정리

1.1 암호학자의 도구 상자

1.2 암호 기술의 종합 응용

1.3 암호와 인증

1.4 암호 기술의 프레임워크화

1.5 암호 기술은 압축 기술

1.1 암호학자의 도구 상자

- **대칭 암호**
- 암호화와 복호화에 같은 키를 이용하는 암호로, 메시지의 기밀성을 지키기 위해 사용
- **공개 키 암호**는 암호화와 복호화에 서로 다른 키를 이용하는 암호로, 대칭 암호와 마찬가지로 메시지의 기밀성을 지키기 위해 사용

- **일방향 해시 함수**는 긴 메시지를 짧은 해시 값으로 변환하는 기술로, 메시지의 무결성을 확인하기 위해 이용
- **메시지 인증 코드**는 통신 상대로부터 온 메시지가 전송도중에 공격자에 의해 수정되어 있지 않다는 것을 확인하는 인증 기술로 메시지의 무결성을 검증하고, 인증을 행하기 위해 이용

- **디지털 서명**은 제3자에 대해 메시지를 검증하고, 통신 상대의 부인 방지를 행할 수 있는 인증 기술
- **의사난수 생성기**는 예측 불가능성을 갖는 비트 열을 생성하는 기술로, 암호나 일방향 해시 함수 등을 사용해서 구성한다. 의사난수 생성기는 키나 초기화 벡터 등을 만들기 위해 사용

암호학자의 도구 상자

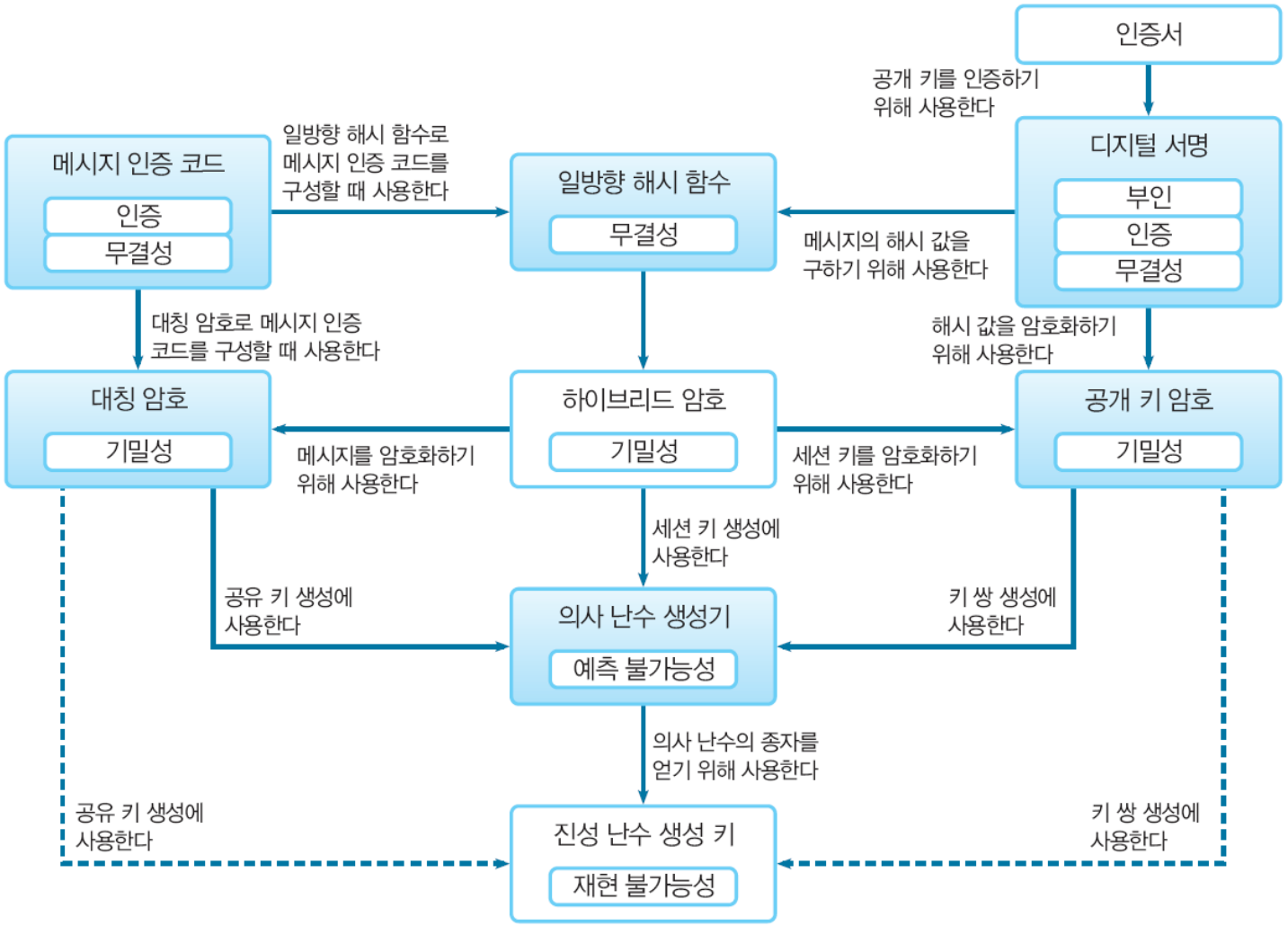

그림 16-1 • 암호학자의 도구 상자

1.2 암호 기술의 종합 응용

- 우리가 지금까지 배운 암호 기술이 아무런 연고나 관계가 없는 두 사람 사이에서 통신을 하게 될 경우에 어떻게 이용되는지를 알아보자

암호기술의 종합 응용

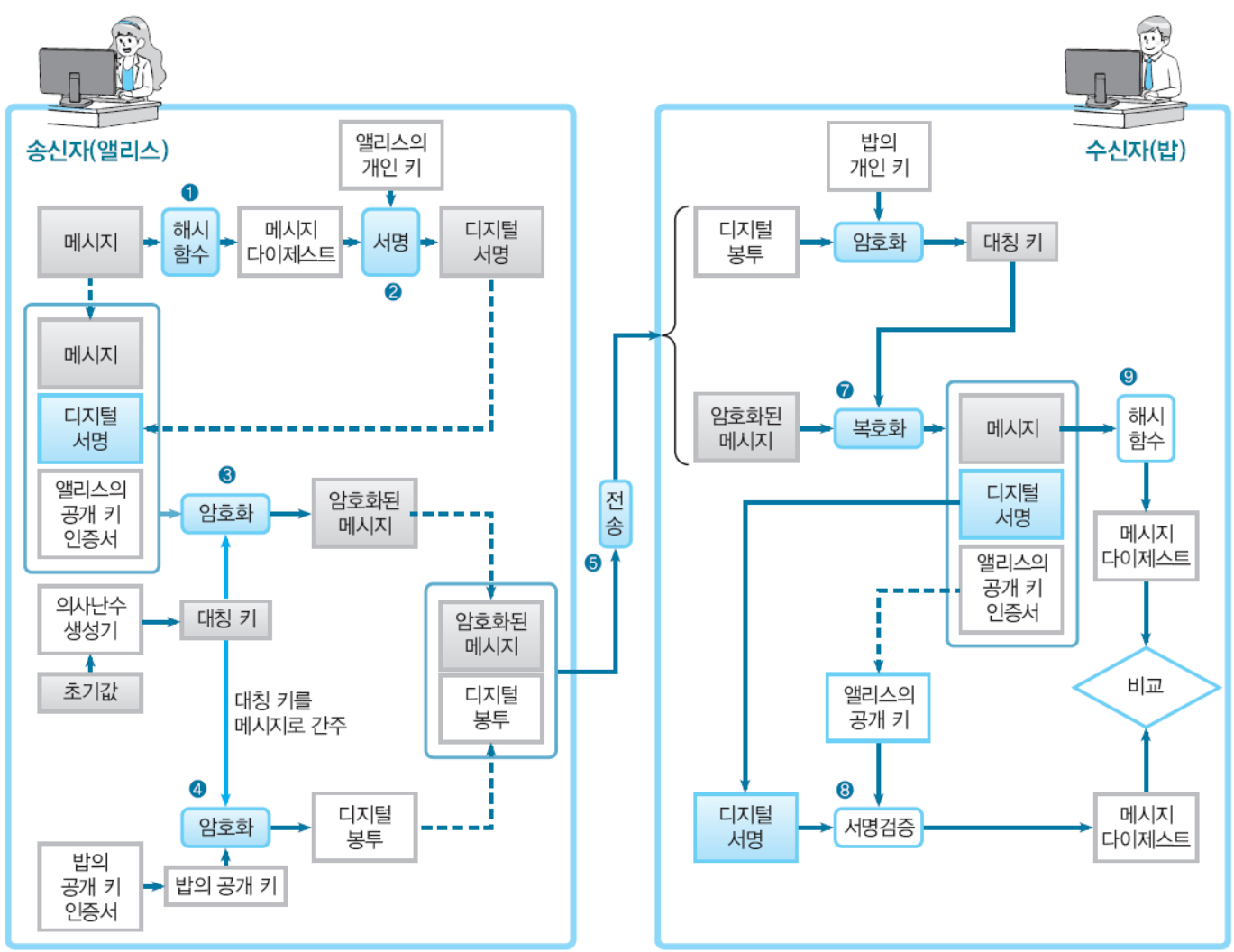

그림 16-2 • 암호 기술의 종합 응용

1.3 암호와 인증

- 「암호」만을 생각하기 쉽지만 암호학자의 도구 상자를 보면 「인증」도 중요

1.4 암호 기술의 프레임워크화

- **프레임워크(framework)**
- 내부에 사용하고 있는 요소 기술을 교환할 수 있는 구조
- 아무리 안전하다고 생각되는 요소 기술이라도, 어느 때 약점이 발견될지 모른다
- 전체가 프레임워크라는 형태로 되어 있으면, 사용하고 있는 개개의 기술에 약점이 발견되었다고 하더라도, 고장 난 부품을 교환하는 것처럼, 그 기술만 교체할 수 있음

1.5 암호 기술은 압축 기술

- 암호학자의 도구 상자 안 기술의 공통점
- 모든 기술이 일종의 「압축 기술」이다
- 「**기밀성의 압축**」
  - 긴 평문을 지키는 대신 짧은 키를 지킨다
- 「**무결성의 압축**」
  - 긴 평문 대신에 짧은 해시 값을 조사
- 「**인증의 압축**」
  - 긴 메시지 대신에 짧은 인증자를 조사

- 「**예측 불가능성의 압축**」
  - 의사난수 열의 예측 불가능성을 이끌어내기 위한 출발점으로서 난수의 종자를 사용

암호 기술은 압축 기술

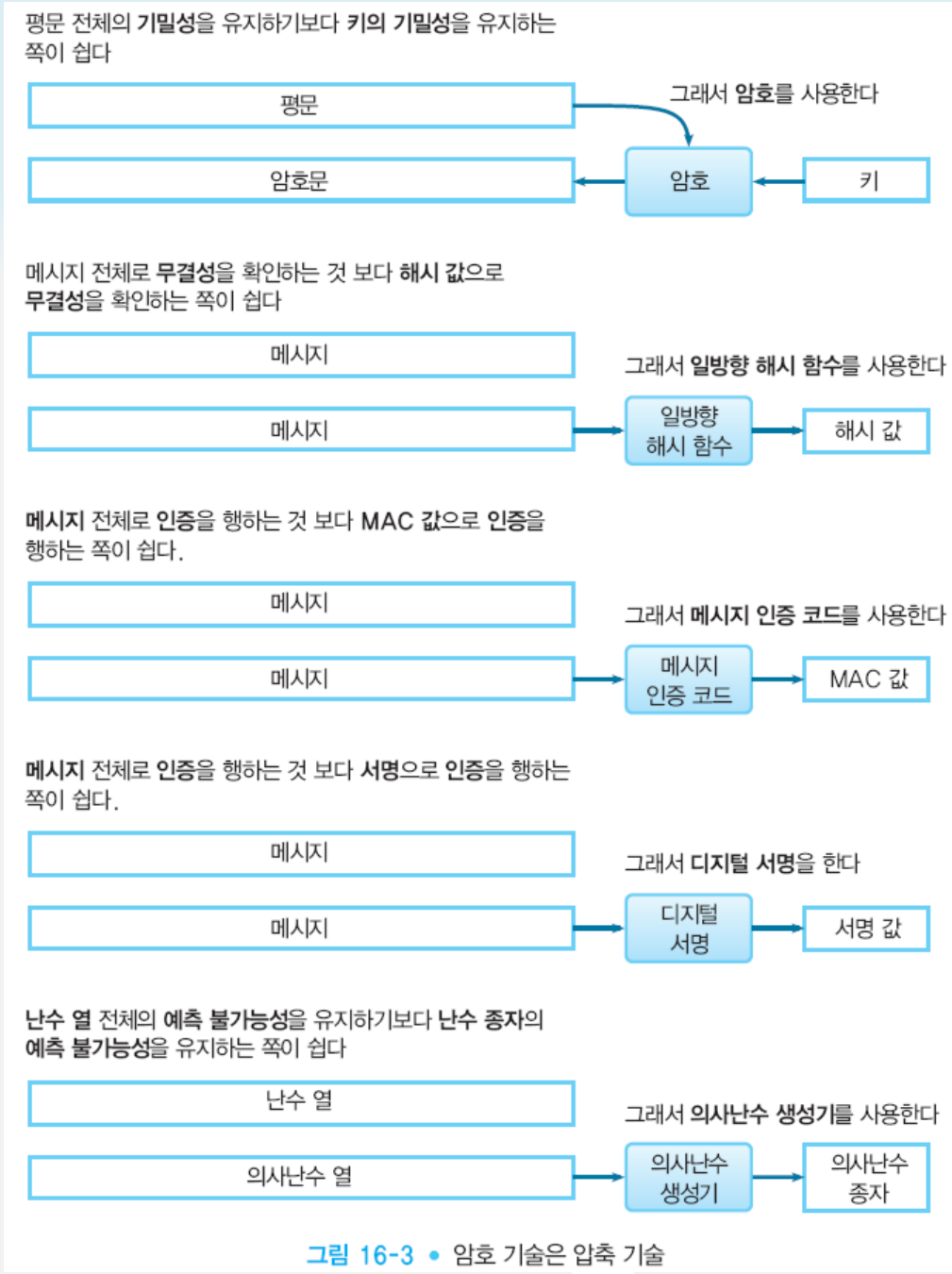

그림 16-3 • 암호 기술은 압축 기술

암호 기술은 압축 기술

표 16-1 암호 기술은 압축 기술

	압축 전	압축 후	특징
대칭 암호	평문	키	기밀성의 압축
공개 키 암호	평문	키	기밀성의 압축
일방향 해시 함수	메시지	해시 값	무결성의 압축
메시지 인증 코드	메시지	인증자(MAC 값)	인증의 압축
디지털 서명	메시지	인증자(서명)	인증의 압축
의사난수 생성기	의사난수 열	종자	예측 불가능성의 압축

Section 02
가상 통화 비트코인

2.1 비트코인이란?
2.2 P2P 네트워크
2.3 어드레스
2.4 월렛
2.5 블록 체인
2.6 블록 추가
2.7 트랜잭션
2.8 채굴
2.9 승인
2.10 익명성
2.11 신뢰의 의미
2.12 비트코인 정리

2.1 비트코인이란

- 비트코인(Bitcoin)
  - 가상통화 또는 암호통화라고 불리는 종류의 하나
  - 물리적으로 떨어져 있더라도 인터넷을 통해 금전의 송수신이 가능
  - 수수료가 저렴하므로 소액 결제도 편리
  - 나까모또 사토시(Nakamoto satoshi)라고 하는 정체불명의 인물이 투고한 논문으로부터 시작
  - 2009년부터 세계 각국에서 사용
  - 2015년에는 미국에서 최초의 비트코인 취급소 코인베이스(Coinbase)가 오픈

비트코인

- 1비트코인은 1 bitcoin 또는 1 BTC로 표현
- 1 satoshi
  - 0.00000001 BTC를 비트코인 원 논문 저자 이름으로 명칭
- 상대적인 가치는 변동
  - 2017년 1월 현재 1BTC는 약 100만원에 해당

비트코인 단위

표 16-2 비트코인의 단위

비트코인	단위(약자)
1	bitcoin (BTC)
0.01	bitcent (cBTC)
0.001	millibitcoin (mBTC)
0.000001	microbitcoin (uBTC)
0.00000001	satoshi

2.2 P2P 네트워크

- 비트코인을 관리하는 중앙은행이 없음
- P2P 네크워크(Peer to Peer Network)
  - 세계의 비트코인 사용자가 구성하는 P2P 네트워크가 비트코인을 통화로 성립시키는 구조
  - 전 세계에 존재하는 비트코인 사용자의 컴퓨터(노드 또는 피어)가 비트코인이라는 시스템을 지원하기 위해 필요한 정보를 확보, 검증
- 비트코인은 P2P 네트워크 상에서 동작하는 결제 시스템
  - 비트코인 사용자는 비트코인이라는 결제 시스템을 사용해서 가치를 이동

2.3 어드레스

- 비트코인의 거래는 **비트코인·어드레스** 사이에서 이루어짐

앨리스가 밥 상점에서 상품 구매 후 비트코인으로 대금지급 방법

- 밥 상점은 어드레스 B를 만든다.
- 밥 상점은 어드레스 B를 앨리스에게 송신한다.
- 앨리스는 어드레스 A를 만든다.
- 앨리스는 어드레스 A로부터 어드레스 B로 상품대금을 지불한다.

어드레스

- 앨리스가 밥에게 메일을 보내는 것과 유사
- 메일이 메일 어드레스 간에 전달되는 것과 같이, 비트코인의 거래는 어드레스 간에 이루어짐
- 메일 어드레스와는 다름
  - 일반적으로 비트코인에서는 거래마다 다른 어드레스를 사용함
  - 기부 등이 목적인 경우에는 동일 어드레스가 여러 번 사용되는 경우도 있음

어드레스

- 공개 키의 해시 값으로부터 작성
- 타원곡선 DSA 공개 키를 일방향 해시함수 SHA-256과 RIPEMD-160 2개를 통해서 해시 값을 구하고, 정보를 부가한 후에 Base58Chek로 부호화해서 문자 열로 변환
- 잘못 읽히는 것을 방지하기 위해 Base58Chek 부호화에서는 숫자 영(0), 대문자 오(O), 대문자 아이(I), 소문자 엘(l)은 사용하지 않음

어드레스 예

- Wikipedia의 창시자 Jimmy Wales가 2014년 3월 7일에 Twitter에 올린 한 어드레스

  1McNsCTN26zkBSHs9fsgUHHy8u5S1PY5q3

- 비트코인 공개 키로부터 만들어진 어드레스(Bitcoin pubkey hash)는 이 예와 같이 "1"로 시작

2.4 월렛

- 월렛(Wallet)
  - 비트코인으로 거래를 할 때 사용하는 비트코인용 어플
  - 자신의 컴퓨터나 스마트폰에 월렛을 설치하거나 Web 서비스로서 제공되고 있는 월렛을 이용해서 비트코인을 사용

월렛

- 월렛을 사용해서 공개 키 쌍을 생성
- 인터넷을 이용해서 거래
- 공개 키
  - 비트코인을 주고받기 위하여 사용
- 개인 키
  - 비트코인을 송금하기 위해 사용
- 월렛 안에는 개인 키가 보존되어 있지만 통상 공개 키 쌍을 취급할 때와 마찬가지로 타인에게 개인 키를 보여주어서는 안 됨

2.5 블록 체인

- **블록 체인(block chain)**
  - 비트코인의 모든 거래가 기록되는 공개 거래 기록부
  - 비트코인을 사용해서 하는 모든 거래는 전 세계에 단 하나의 공개거래기록부에 기록
  - 블록 체인이라는 이름이 주는 의미처럼 복수의 거래는 **블록(block)**이라는 단위로 정리

블록 체인

그림 16-4 • 블록 체인

블록 체인의 기능

- 예: 앨리스의 어드레스A로부터 밥의 상점 어드레스 B에 대해 1 BTC를 지급하는 것의 의미
  - 어드레스 A가 지불할 수 있는 비트코인이 1 BTC 감소한다
  - 어드레스 B가 지불할 수 있는 비트코인이 1 BTC 증가한다

2.6 블록 추가

- **트랜잭션(transaction)**
  - 비트코인 거래 단위
  - 다른 트랜잭션과 함께 1개의 블록에 정리되어진 후 블록 체인에 추가
  - P2P 네트워크가 추가를 승인하면 트랜잭션에 대응하는 거래가 성립

블록 체인 구성 과정

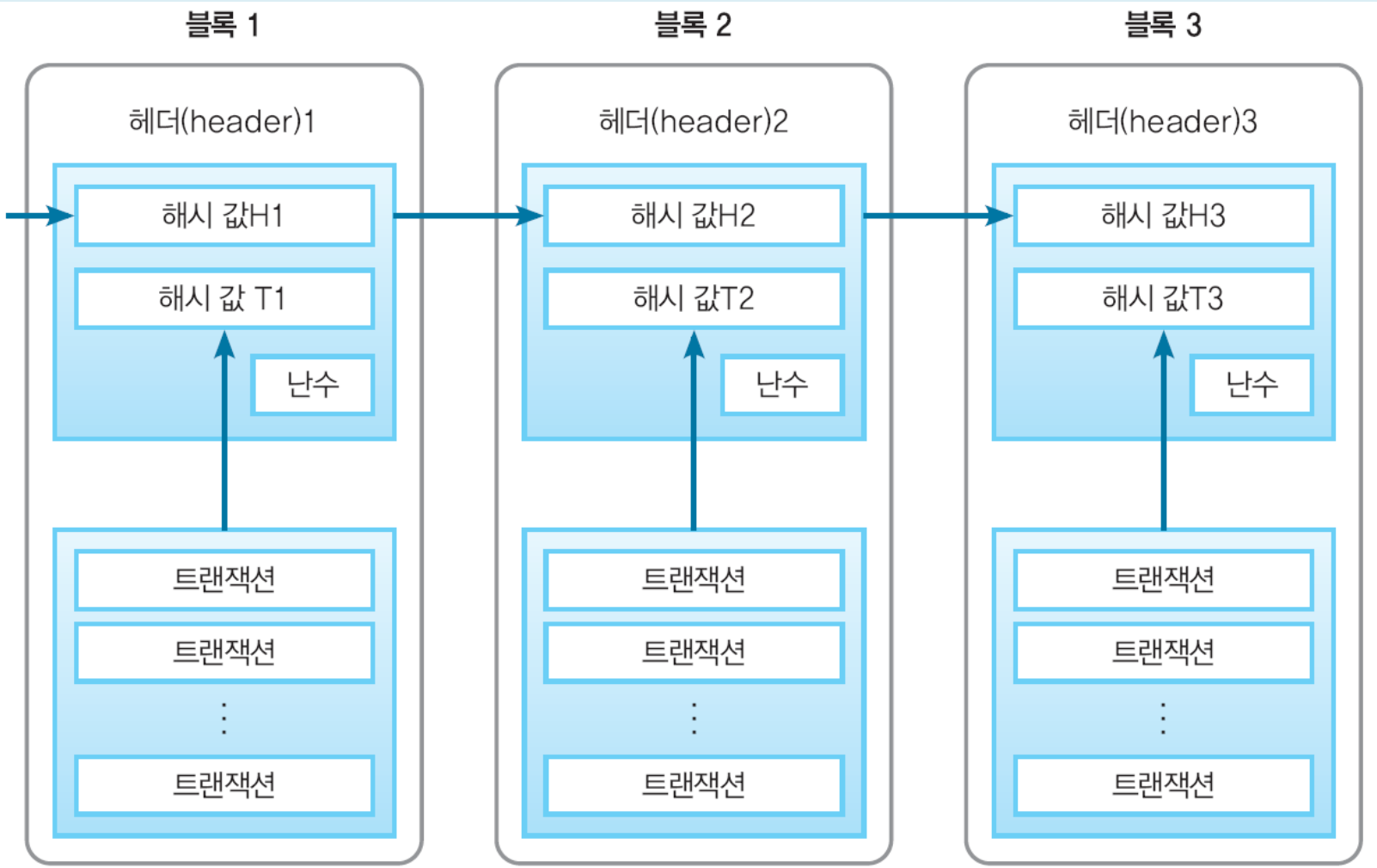

그림 16-5 • 블록 체인

블록 구성

- 블록(Block)
  - 트랜잭션 집합과 헤더(header)로 구성
  - 헤더
    - 직전 블록의 헤더의 해시 값이 보존
    - 트랜잭션의 집합 전체의 해시 값」도 보존
    - 난수라고 불리는 임의의 값이나 타임스탬프(그림에서는 생략) 등도 보존

2.7 트랜잭션

- **트랜잭션(transaction)**
  - 「어느 어드레스로부터 별개의 어드레스에 어느 비트코인을 보내는가」, 즉, 「거래」를 기록한 것
  - 예:
  - 앨리스가 밥 상점으로부터 상품을 사고, 앨리스는 밥의 상점에 비트코인 1BTC를 상품대금으로 지불

블록 체인 안의 해시값 역할

- 블록 체인을 조금이라도 바꿔 쓰면 그 이후의 모든 블록 헤더를 변경해야만 함
- 블록헤더에 포함되어 있는 2개의 해시 값은 블록 체인의 내용 변경을 어렵게 하는 효과

지불 과정

- 밥 상점
  - 공개 키 쌍(공개 키 *B* 와 개인 키 *b*)을 작성
  - 공개 키 *B* 로부터 어드레스 B를 만들고, 앨리스에게 전달
- 앨리스
  - 공개 키 쌍(공개 키*A* 와 개인 키 *a*)를 작성
  - 「어드레스 A로부터 어드레스 B로의 1BTC 송금」이라는 트랜잭션을 만든다. 이때 개인 키 *a* 를 사용해서 디지털 서명을 작성
  - 그 트랜잭션을 P2P 네트워크로 송신. 즉, 이 거래를 전 세계에 브로드 캐스트 한다.
  - 앨리스가 만든 트랜잭션은 다른 트랜잭션과 함께 블록에 정리되고, 블록 체인에 추가 됨
  - 추가된 블록이 P2P 네트워크로부터 승인되면, 「어드레스 A로부터 어드레스 B에 대해서 1BTC 송금」이라는 거래가 성립한 것

지불 과정의 보안성

- A가 앨리스라는 사람의 어드레스라는 것과, B가 밥의 상점의 어드레스라는 것 자체는 공개적으로 알려지지 않음
- 그러나 앨리스는 오직 밥의 상점에 지불하고 싶고, 밥의 상점은 앨리스로부터 지불을 받기를 원하므로, 이 트랜잭션은 누구로부터 누구의 송금인지, 앨리스와 밥의 상점은 서로 알 필요가 없음
- 이 거래는 SNS나, 메일, Web 사이트 등 비트코인의 시스템 외에서 행하는 것

블록을 구성하는 트랜잭션

- 트랜잭션이 블록에 모아지고, 블록 체인에 추가된 것에 의해, 어드레스 A가 지불할 수 있는 금액은 1BTC 감소하고, 어드레스 B가 지불할 수 있는 금액은 1BTC 증가
- 트랜잭션을 작성
  - 디지털 서명 기술이 사용
- 비트코인에서 사용되고 있는 디지털 서명 알고리즘
  - 타원곡선 DSA로 방정식 $y^2 = x^3 + 7$의 타원곡선이 사용

2.8 채굴

- 지불을 하려면 최초의 어드레스가 필요
  - 블록 체인에 블록을 추가하는 행위가「지불 가능한 어드레스를 새롭게 만드는 행위」
- 채굴(mining)
  - 블록 체인에 블록을 추가하는 것을 비트코인을 금광으로부터 채굴하는 것에 비유
- 채굴자(miner)
  - 채굴하는 사람

블록 체인

- 1개의 사슬과 같으므로 어느 순간에 추가할 수 있는 블록은 1임
- 보수(block reward)
  - 블록을 추가한 채굴자에게 주어지는 보상
- 트랜잭션 수수료(transaction fee)
  - 그 블록에 포함되는 트랜잭션으로부터 받는 보상
- 프로토콜로 관리
  - 채굴에 의한 보수
  - 2012년까지는 50BTC
  - 2015년에는 25BTC(당시 약 750만원)
  - 2016년 7월 이후는 12.5BTC

PoW(Proof of Work)

- 비트코인의 위조를 방지하기 위하여 채굴자는 자신의 정당한 분량의 작업을 한 것을 증명하여야 하는 데 이를 PoW라 함
- PoW를 실현하기 위해 해시 값 활용
  - 직전 헤더 해시 값은 상위 비트에 다수개의 0이 나열되는 패턴이 되어야 함
  - 예:

000000000000000000007780B6F7817C431309EDED44F51223352D86A4436023913

  - 이런 해시 값을 구하려면 엄청난 컴퓨팅 계산 능력이 필요함

2.9 승인

- 많은 채굴자가 전 세계에서 블록을 추가하려고 시도
- 블록이 추가되는 것은 분기가 이뤄지는 것
- 승인
  - 블록 체인에 어느 블록을 올바른 것으로 추가해야 하는지를 판단하는 것이 P2P 네트워크에 의한 승인임

블록 체인 분기

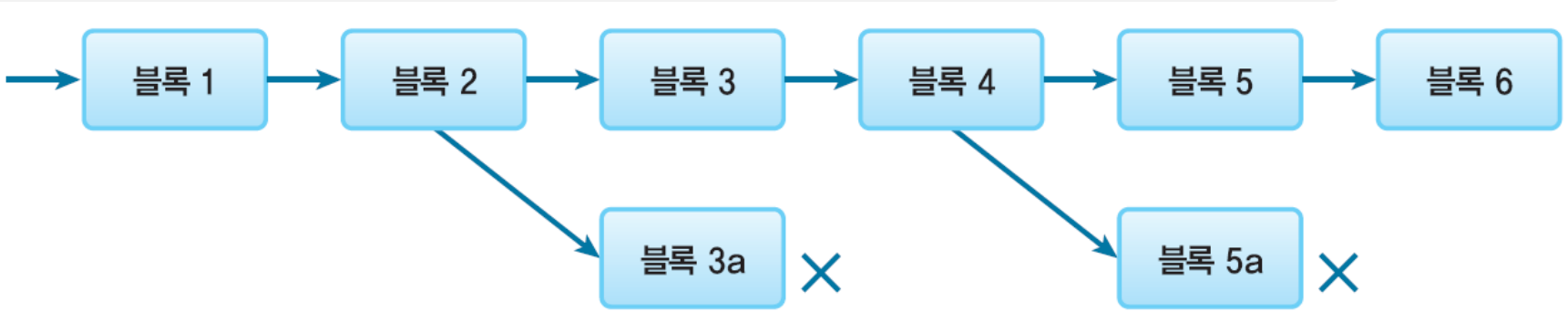

그림 16-6 • 블록 체인의 분기

2.10 익명성

- 월렛에서 어드레스를 만들 때 자신의 이름이나 메일 어드레스를 관련 지을 필요가 없음
- 거래를 하는 상대방에게 자신의 이름이나 메일 어드레스가 알려질 리 없음
- 그런 의미에서는 분명히 비트코인의 거래는 익명

익명성

- 모든 어드레스로 행하는 거래는 전 세계에 알려지게 됨
- 거래 기록은 반영구적으로 블록 체인 상에 계속해서 보존
- 통상 1개의 어드레스로 중복 해서 거래하지 않는다

익명성

- 상거래를 한다고 하는 것은 상품을 배달받기 위하여 신원을 어느 정도 밝혀야 된다
- 거래 상대방이 「이 어드레스는 앨리스의 것이다!」라고 공개해 버리면, 그 어드레스로 거래되는 것을 전 세계에 알리는 것이 된다.
- 더욱이 P2P 네트워크라는 성질상 어느 거래에 관련하여 노드의 IP 어드레스가 기록되는 위험성도 있다

블록 체인 열람

- Blockchain.info라는 사이트에서는 블록 체인을 열람

2.11 신뢰의 의미

- 비트코인에서 다음의 의미를 알아보자
  1. 비트코인을 통해서 지불하는 상대를 신뢰하는 것
  2. 비트코인 거래소를 신뢰하는 것
  3. 비트코인 시스템을 신뢰하는 것

비트코인을 통해서 지불하는 상대를 신뢰하는 것

- 현금으로 물건을 사는 상대를 신뢰하는 것과 유사
- 상대에게 비트코인으로 지불할 때 약속한 상품이 배달되리라는 신뢰를 할 수 있는가 여부임
- 비트코인은 현금과 유사
- 현금을 상대방에게 건넬 때 상대방이 갖고 도망가버리면 어쩔 도리가 없음

비트코인 거래소를 신뢰하는 것

- 현금을 예치하는 은행을 신뢰하는 것과 유사
- 송금 시간을 감소시키기 위해, 또는 다른 통화와의 교환을 위해 비트코인을 취급하는 거래소가 수 많이 운영되고 있음
- 예로, 비트코인 시스템을 신뢰할 수 있다 하더라도, 거래소가 도난 당하거나 사기를 칠 가능성이 있음
  - 실제 2014년에 거대한 거래소 마운트고크스에서 수천억 원이 없어져 버리는 사건이 발생

비트코인 시스템을 신뢰하는 것

- 비트코인에서 사용되는 암호기술이나, 그 암호기술을 내장하고 있는 월렛 등의 소프트웨어를 신뢰하는 것
- 암호기술을 기반으로 하여 모두 오픈해서 만들어진 것이고, 거기에 숨겨진 시큐리티(security by obscurity)는 없으므로「신뢰」할 수 있음

2.12 비트코인 정리

- P2P 네트워크에 의해 만들어진 결제시스템으로 거래는 공개 키로부터 만든 어드레스 간에 행한다.
- 송금이 바르다라고 하는 것은, 송신자가 개인 키를 사용해서 행하는 디지털 서명에 의해 나타난다.
- 일방향 해시 함수를 사용해서 블록 체인이라는 공개 거래장부에 모든 거래가 기록되어 있고, 그 정합성은 아무나 검증할 수 있다(투명성).
- PoW(Proof of Work)로 위조나 블록 체인 분기를 방지
- 블록을 추가하기 위하여 채굴자는 상위 비트에 0이 나열되는 값이 보일 때까지 해시 값 계산을 반복한다(채굴). 블록을 추가하면 보수로서 비트코인을 얻는다.

Section 03
완전한 암호 기술을 꿈꾸며

3.1 양자 암호

3.2 양자 컴퓨터

3.3 어느 쪽이 먼저 실용화될까?

3.1 양자 암호

- **양자 암호(quantum cyrptography)**
  - 양자론을 이용한 암호 기술로
  - 베넷(Bennett)과 브라사르(Brassard)에 의해 1980년대에 제안
  - 「암호」라고 이름이 붙어 있지만, 엄밀하게는 암호를 직접 구성하는 것이 아니라, 도청이 불가능한 통신을 구성하는 기술
  - 광자의 양자론적인 성질을 이용한 통신 방법

양자 암호의 특징

- **광자가 진동하는 방향을 정확하게 측정하는 것이 원리적으로 불가능하다는 사실**
  - 이 사실은 도청한 내용을 부정확하게 할 수 있다고 하는 결과를 낳는다.
- **측정하는 것으로 광자의 상태가 변화된다는 사실**
  - 이 사실은 도청이 이루어지면 수신자가 도청 사실을 알 수 있다는 결과를 낳는다.

양자암호 프로토콜

- BB84 프로토콜:
  - 네 개의 양자상태로 1비트의 정보를 표현
- B92 프로토콜:
  - 두 개의 양자상태로 1비트의 정보를 표현
- E91 프로토콜:
  - BB84 프로토콜과 같지만 서로 뒤얽히는 일련의 광자대를 이용
  - 한쪽의 광자를 측정하면 원격지에 있는 광자의 상태가 확정된다는 양자적인 현상을 이용

양자암호통신 실험

- 32cm 거리:
  - 1989년; 미국; 양자 암호 통신에 성공
- 87km 거리
  - 2002년; 일본; 미츠비시전기; 양자 암호 통신에 성공
- 200Km 거리
  - 2007년에는 NTT 연구소의 이노우에:
  - 차동위상(differential phase) 시프트 양자 키 배송(DPS-QKD) 방식으로 양자키를 광섬유를 통해 전송하는 데 성공
- 307Km 거리
  - 2015년에 제네바 대학과 코닝사에서 광섬유를 이용한 양자 키 전송 성공

3.2 양자 컴퓨터

- 양자 암호가 암호학자의 궁극적인 도구가 된다면, **양자 컴퓨터**는 암호해독자의 궁극적인 도구
- 양자 컴퓨터는 양자 암호와 같이 양자론을 이용한 기술로 1985년 영국의 데이비드 도이치(David Deutsch)에 의해 제안
- 현재까지 양자 컴퓨터 실용화는 미해결

3.3 어느 쪽이 먼저 실용화 될까?

- 양자 암호가 양자 컴퓨터보다도 먼저 실용화되면, 양자 암호를 사용해서 일회용 패드를 구축하고, 완전한 암호 기술이 탄생
- 양자 암호보다도 앞서 양자 컴퓨터가 탄생하면, 현재의 암호 기술에 의한 암호문은 모두 해독

04: 완전한 암호 기술과 불완전한 인간

4.1 이론은 완전하더라도 현실은 불완전하다

4.2 방어는 완전하지 않으면 안 되지만, 공격은 어느 한 곳만 깨면 된다

4.3 공격 예 1: PGP로 암호화된 메일에 대해

4.4 공격 예 2: SSL/TLS로 암호화된 신용카드 번호에 대해

Section 04

완전한 암호 기술과 불완전한 인간

4.1 이론은 완전하더라도 현실은 불완전하다

4.2 방어는 완전하지 않으면 안 되지만, 공격은 어느 한 곳만 깨면 된다

4.3 공격 예 1: PGP로 암호화된 메일에 대해

4.4 공격 예 2: SSL/TLS로 암호화된 신용카드 번호에 대해

4.1 이론은 완전하더라도 현실은 불완전하다

- 암호 이론은 수학적 근거를 가지고 있거나 논리적이라 믿을만해 보인다
- 암호 알고리즘 구현은 컴퓨터를 통해 이루어지므로 신뢰할 수 있는 것처럼 보인다
- 이론적 완전성과 현실적인 완전성은 그 의미가 다르다

4.2 방어는 완전하지 않으면 안되지만, 공격은 어느 한 곳만 깨면 된다

- 방어:
  - 시스템을 방어하기 위해서는 공격자의 온갖 공격에 대비
- 공격:
  - 시스템 공격에서 유효한 공격 단 한 가지 방법만 찾아내면 충분
  - 방어하는 쪽 한 순간의 허점을 찌르는 것만으로도 공격에 성공

한 명만 취약해도 실패

- 강력한 암호나 인증을 갖춘 시스템이 있고, 1000명 중 999명은 보안의식이 높아도, 나머지 한 명이 관리를 제대로 하고 있지 않다면, 그 사람을 발판으로 해서 침입할 가능성이 있다.
- 공격자는 시스템 중 가장 약한 부분 한 곳만 깨면 충분

4.3 공격 예 1: PGP로 암호화된 메일에 대해

- **사회 공학**(Social Engineering) 공격
  - 암호 기술을 정면으로 공격하기보다도 효과적인 공격
  - 심리를 이용한다
    - 매수
    - 폭력
    - 회유
  - 암호의 강도와는 무관한 공격방법

앨리스 행세로 메일 보내기

밥에게

있지, 이 게임 한 적 있니?

굉장히 재미있어.

메일에 첨부한다. 더블 클릭하면 바로 시작돼.

실은 맬로리

↓

앨리스로부터

[첨부 파일 : funnygame.exe]

게임 실행 순간 메일 소프트웨어에 다른 프로그램이 몰래 설치

4.4 공격 예 2: SSL/TLS로 암호화된 신용카드 번호에 대해

- 맬로리는 앨리스의 컴퓨터에 침입해서, 파일을 찾고, 앨리스가 무심코 어딘가에 기록한 신용카드 번호를 찾아내려는 시도를 한다
- 피싱 사이트 이용
- 가용성에 대한 공격
  - 서비스 거부 공격(DoS: Denial of Service)
  - 분산 서비스 거부 공격(DDoS: Distributed Denial of Service)