



BitCoin and BlockChain

2017.10.28

Jaeyun Kang

비트코인과 블록체인

비트코인? 블록체인? 많이 들어보긴 했는데 애네들이 뭐지?



?



BLOCKCHAIN

화폐란?



거래: 서로가 가치 있다고 믿는 물품의 교환

과거의 거래 방식: 물물교환

'가치'를 대변하는 '표준'의 필요성 -> 화폐!

화폐의 변화



금

화폐의 변화



금



지폐

화폐의 변화



금



지폐



가상화폐 ?

제3의 '중앙 기관'에 의존하지 않는 화폐
인터넷상에서 자유롭게 사용가능한 화폐

가상화폐



가상화폐 ?

제3의 '중앙 기관'에 의존하지 않는 화폐
인터넷상에서 자유롭게 사용가능한 화폐

일반화폐는?



발행: 중앙은행



신한은행



기업은행



KB 국민은행

전자화폐 장부: 각 시중 은행 인터넷 뱅킹 서비스

가상화폐



가상화폐 ?

제3의 '중앙 기관'에 의존하지 않는 화폐
인터넷상에서 자유롭게 사용가능한 화폐

일반화폐는?



발행: 중앙은행
화폐의 가치를 담보



신한은행



IBK 기업은행



KB 국민은행

전자화폐 장부: 각 시중 은행 인터넷 뱅킹 서비스
장부의 신뢰성을 담보

가상화폐



가상화폐 ?

제3의 '중앙 기관'에 의존하지 않는 화폐
인터넷상에서 자유롭게 사용가능한 화폐

일반화폐는?



발행: 중앙은행
화폐의 가치를 담보
부패?



신한은행



기업은행



KB 국민은행

전자화폐 장부: 각 시중 은행 인터넷 뱅킹 서비스
장부의 신뢰성을 담보
해킹?

가상화폐



화폐의 발행 & 거래장부 기록을 모두 P2P 분산 네트워크 상에서!
탈중앙화

가상화폐



화폐의 발행 & 거래장부 기록을 모두 P2P 분산 네트워크 상에서!
탈중앙화

해결해야 될 문제점

어떻게 사용자를 인증할 것인가?

어떻게 이중지불을 방지할 것인가?

어떻게 장부조작을 방지할 것인가?

비트코인은 이 물음들의 해답을 최초로 제시!

비트코인의 사용자 인증



Q. 어떻게 사용자를 인증할 것인가?

강재윤이 비트코인 30BTC를 계좌에 보유하고 있다고 하자.
계좌번호는 ABCDX123이다.

누군가 시스템에 들어가 ABCDX123 의 계좌에서 다른 계좌로 30BTC를 송금한다.
라는 거래를 추가 시켰다. 강재윤은 돈을 다 잃는다!

어떻게 계좌의 주인인 '강재윤'만이 계좌의 비트코인을 사용할 수 있게 하는가?

가상화폐 ?

제3의 '중앙 기관'에 의존하지 않는 화폐
인터넷상에서 자유롭게 사용가능한 화폐

비트코인의 사용자 인증



Q. 어떻게 사용자를 인증할 것인가?

강재윤이 비트코인 30BTC를 계좌에 보유하고 있다고 하자.
계좌번호는 ABCDX123이다.

누군가 시스템에 들어가 ABCDX123의 계좌에서 다른 계좌로 30BTC를 송금한다.
라는 거래를 추가 시켰다. 강재윤은 돈을 다 잃는다!

어떻게 계좌의 주인인 '강재윤'만이 계좌의 비트코인을 사용할 수 있게 하는가?

가상화폐 ?

제3의 '중앙 기관'에 의존하지 않는 화폐
인터넷상에서 자유롭게 사용가능한 화폐

공개키 암호화 방식!

비트코인의 사용자 인증

Jaeyun Public Key



Jaeyun Private Key



Jaeho Public Key



Jaeho Private Key



Bjaeho Public Key



Bjaeho Private Key



비트코인의 사용자 인증

Jaeyun Public Key



Jaeho Public Key



Bjaeho Public Key



Jaeyun Private Key



Jaeho Private Key



Bjaeho Private Key



Public Key 로 접근 내용은 대응되는 Private Key로만 풀 수 있다!



비트코인의 사용자 인증

Jaeyun Public Key



Jaeho Public Key



Bjaeho Public Key



Jaeho Public Key



Jaeyun Private Key



Jaeho Private Key



Bjaeho Private Key



Public Key 로 접근 내용은 대응되는 Private Key로만 풀 수 있다!



비트코인의 사용자 인증

Jaeyun Public Key



Jaeho Public Key



Bjaeho Public Key



Jaeho Public Key



Jaeho Public Key



Jaeyun Private Key

Jaeho Private Key

Bjaeho Private Key

Public Key 로 접근 내용은 대응되는 Private Key로만 풀 수 있다!

비트코인의 사용자 인증

Jaeyun Public Key



Jaeho Public Key



Bjaeho Public Key



Jaeho Public Key



Jaeho Public Key



Jaeyun Private Key

Jaeho Private Key

Bjaeho Private Key

Jaeho Private Key를 가진 Jaeho만 받은 돈을 사용할 수 있다!

비트코인의 거래유효성 입증



가상화폐 ?

제3의 '중앙 기관'에 의존하지 않는 화폐
인터넷상에서 자유롭게 사용가능한 화폐

Q. 어떻게 이중지불을 방지할 것인가?

강재윤이 1BTC를 계좌에 보유하고 있다고 하자.

어느날 강재윤이 '방재호'에게 밥을 얻어먹고 1BTC를 송금하고
1일 후 '김재호'에게 밥을 얻어먹고 1BTC를 송금하였다.

나중에 이와 같은 사실이 밝혀지고 강재윤은 파산신청을 했다.

'김재호'는 '방재호'에게 내가 나이가 더 많으니 1BTC는 자신의 것이라고 주장한다.
'방재호'는 억울하다.

**강재윤의 두 번째거래는 유효하지 않다.
어떻게 이를 실행전에 파악하여 막을 것인가?**

비트코인의 이중지불 방지



일반적인 전자화폐 거래에서는

첫번째 거래가 성사되는 즉시 해당 거래가 은행장부에 기록된다.
두번째 거래 요청이 들어왔을 시에, 은행은 거래 장부를 통해
강재윤의 잔고가 부족함을 확인할 수 있고
두번째 거래가 유효하지 않다고 검증한다!

이 모든것은 '은행' 이라는 중앙거래기관이 '장부'를 관리하기 때문!

가상화폐 ?

제3의 '중앙 기관'에 의존하지 않는 화폐
인터넷상에서 자유롭게 사용가능한 화폐

비트코인의 이중지불 방지



그러나, **분산장부**에서는..?

하나의 합의된 장부를 유지해야만 한다!

그렇다면 비트코인은 어떻게 합의된 장부를 유지하는가?

비트코인에에서 이러한 합의된 장부를 '**블록체인**'이라 하며

블록체인을 만드는 사람들을 '**채굴자**'라 한다.

가상화폐 ?

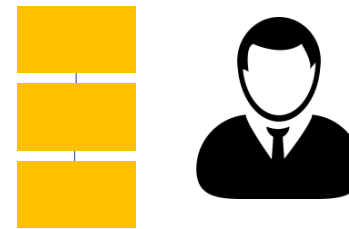
제3의 '중앙 기관'에 의존하지 않는 화폐
인터넷상에서 자유롭게 사용가능한 화폐

비트코인과 블록체인



채굴자

블록체인



블록체인

채굴자



채굴자

블록체인

채굴자
= 블록을 생성하는 사람들
= 거래를 검증하는 사람들

블록체인은 현재까지 모두
합의된 상태라고 가정하자!



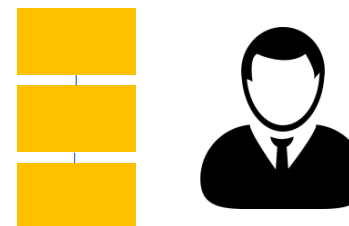
블록체인

채굴자



채굴자

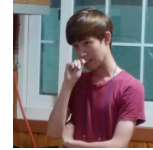
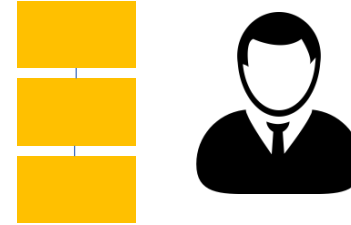
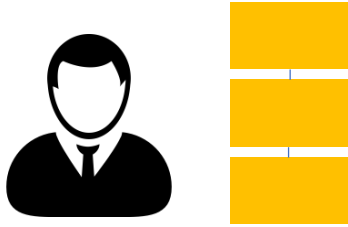
블록체인



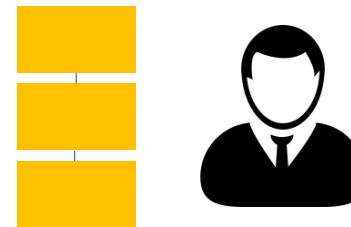
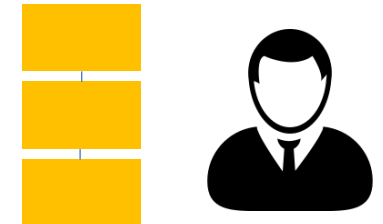
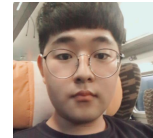
블록체인

채굴자

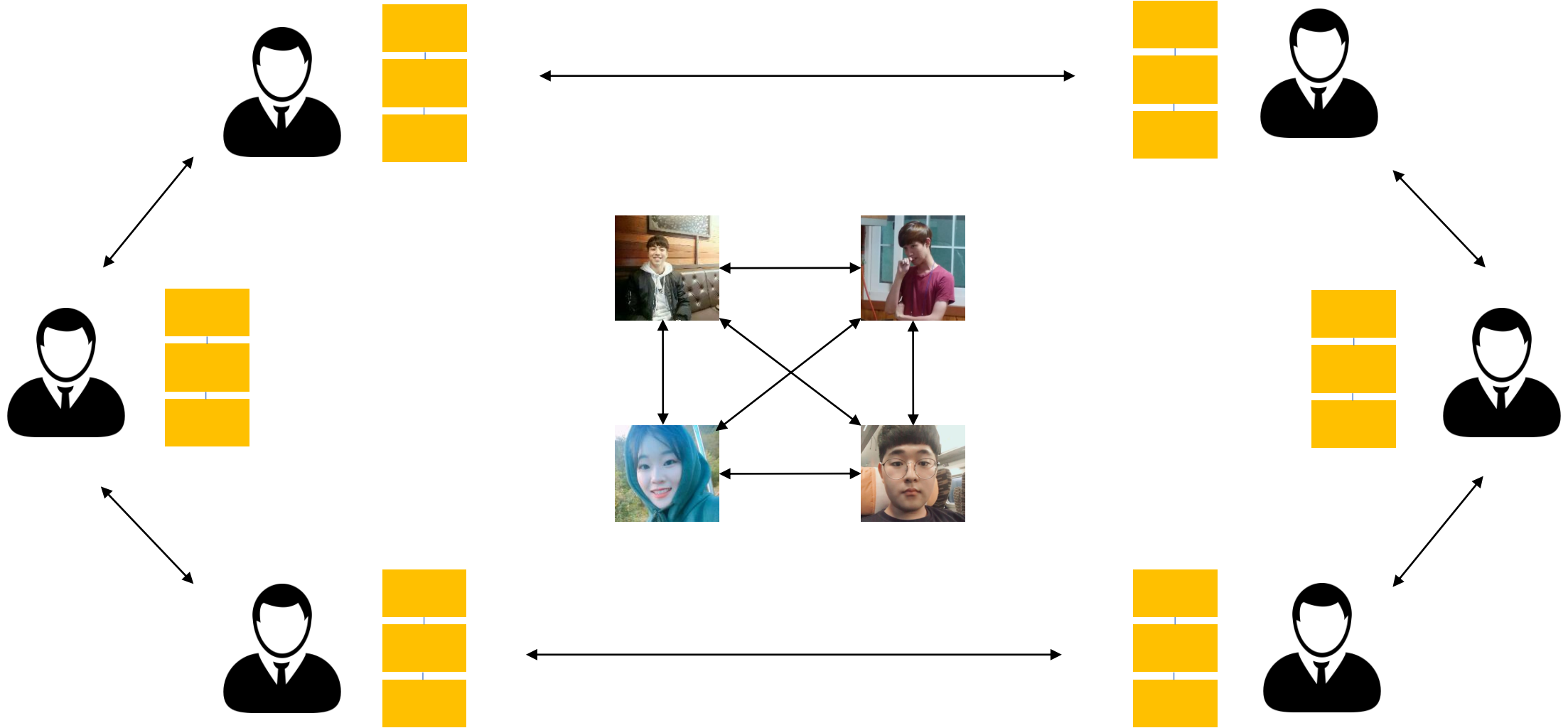
비트코인과 블록체인



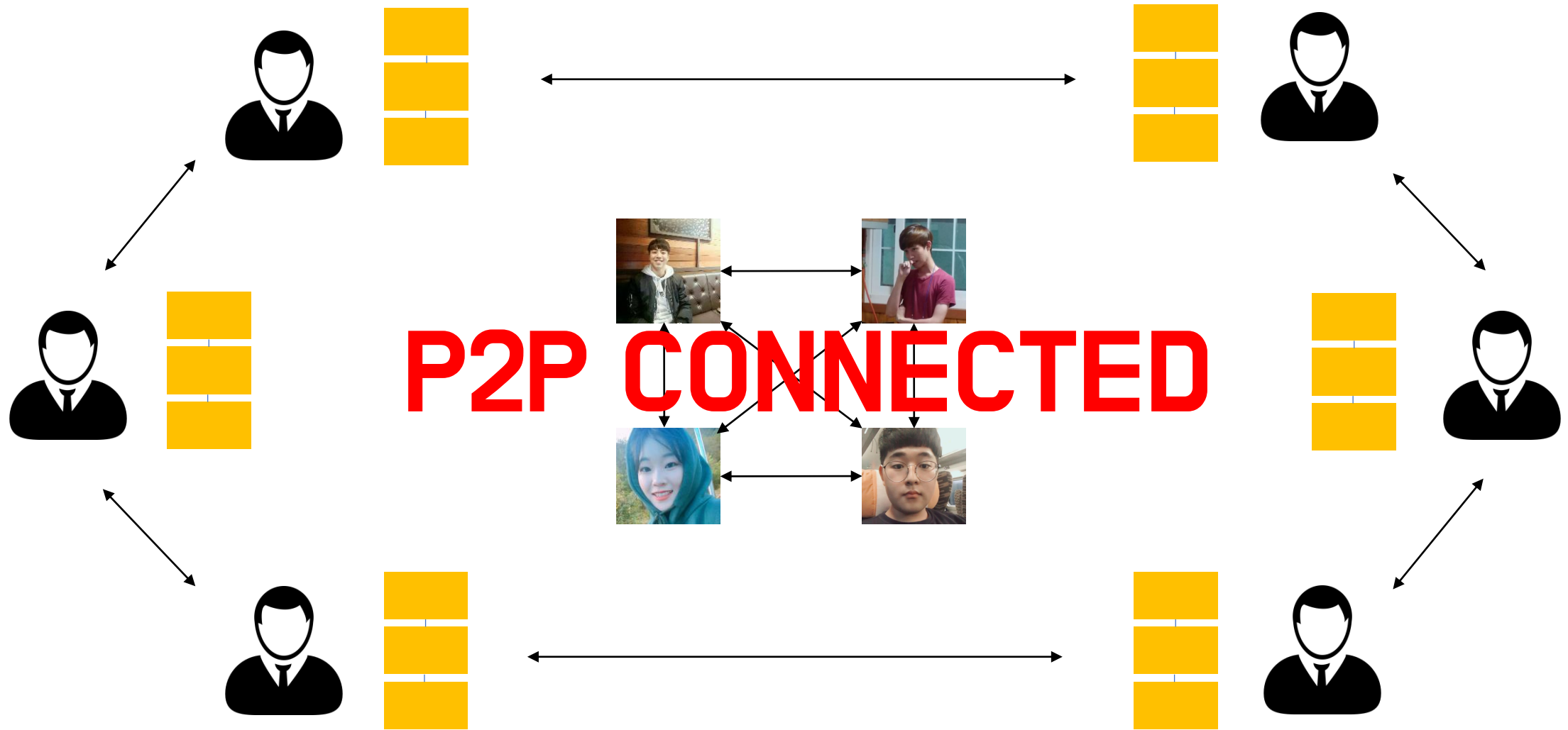
비트코인 이용자



비트코인과 블록체인



비트코인과 블록체인



비트코인과 블록체인

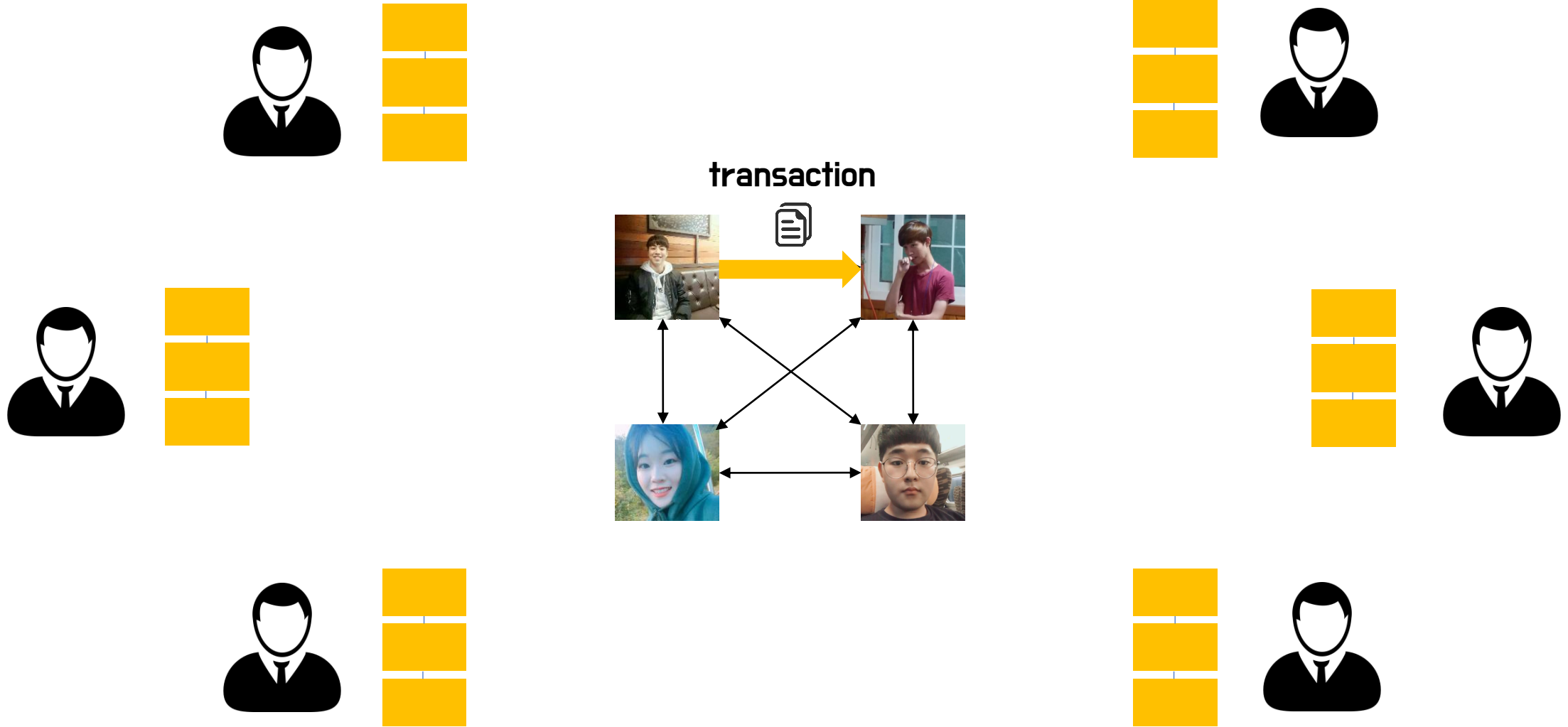


From: 강재윤
To: 김재호
1,000 BTC

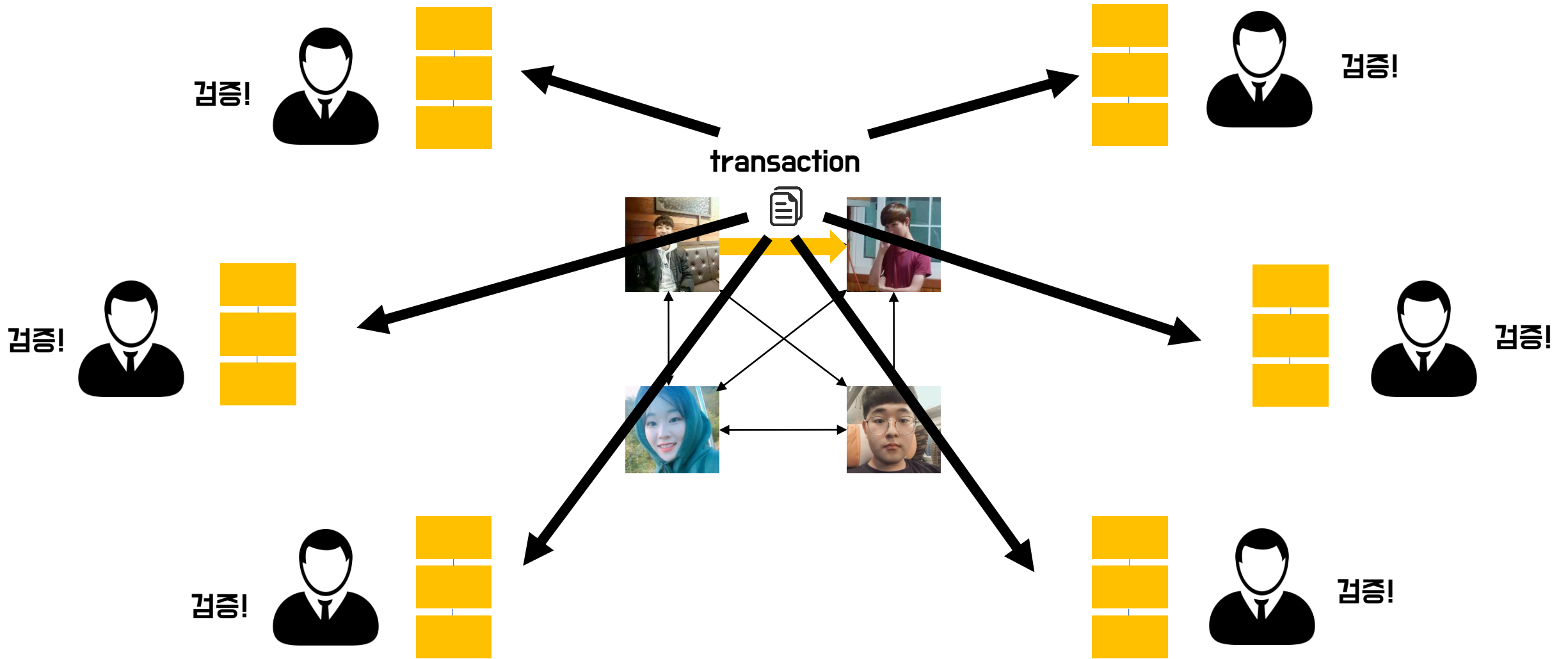


= Transaction

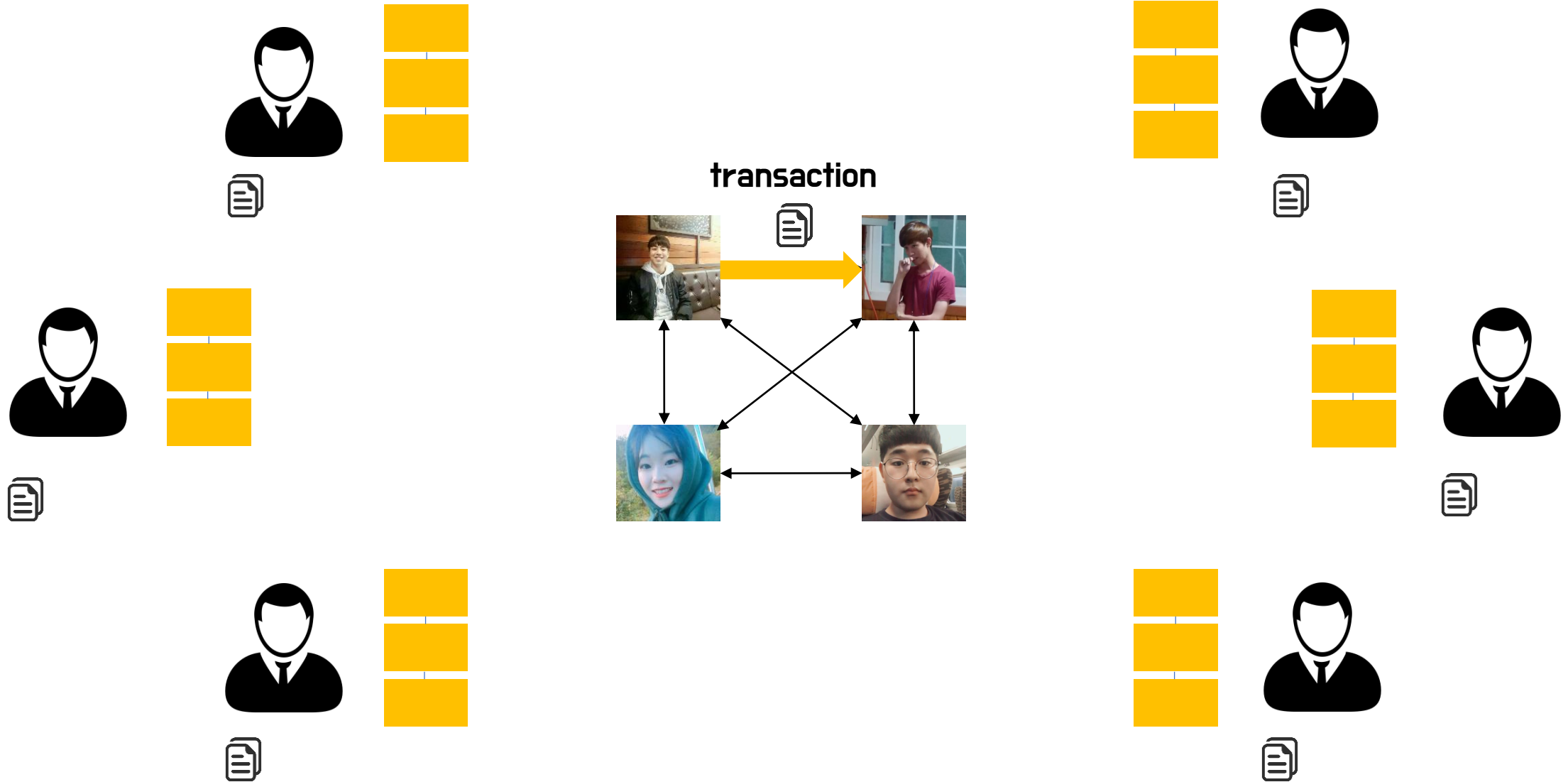
비트코인과 블록체인



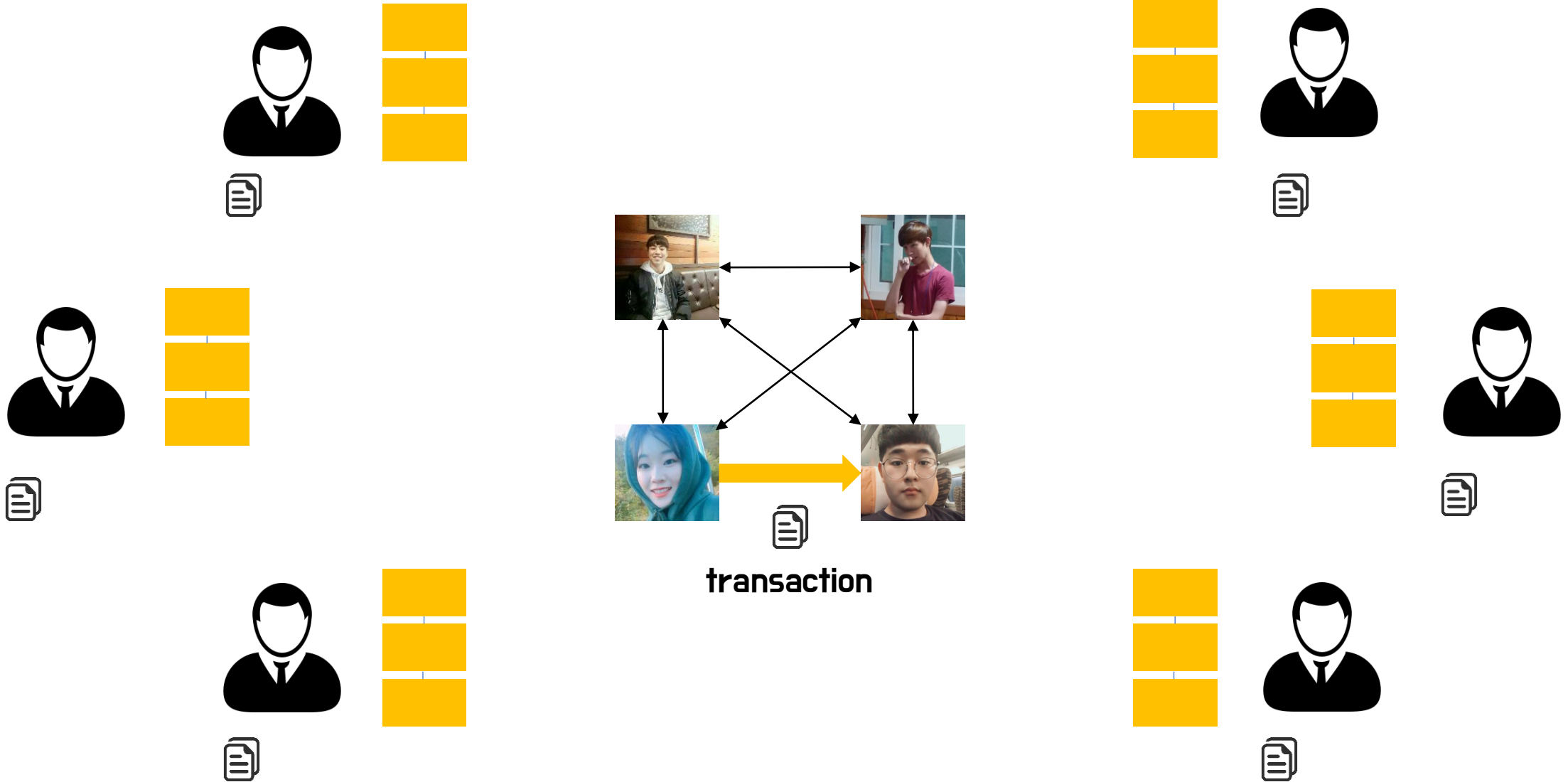
비트코인과 블록체인



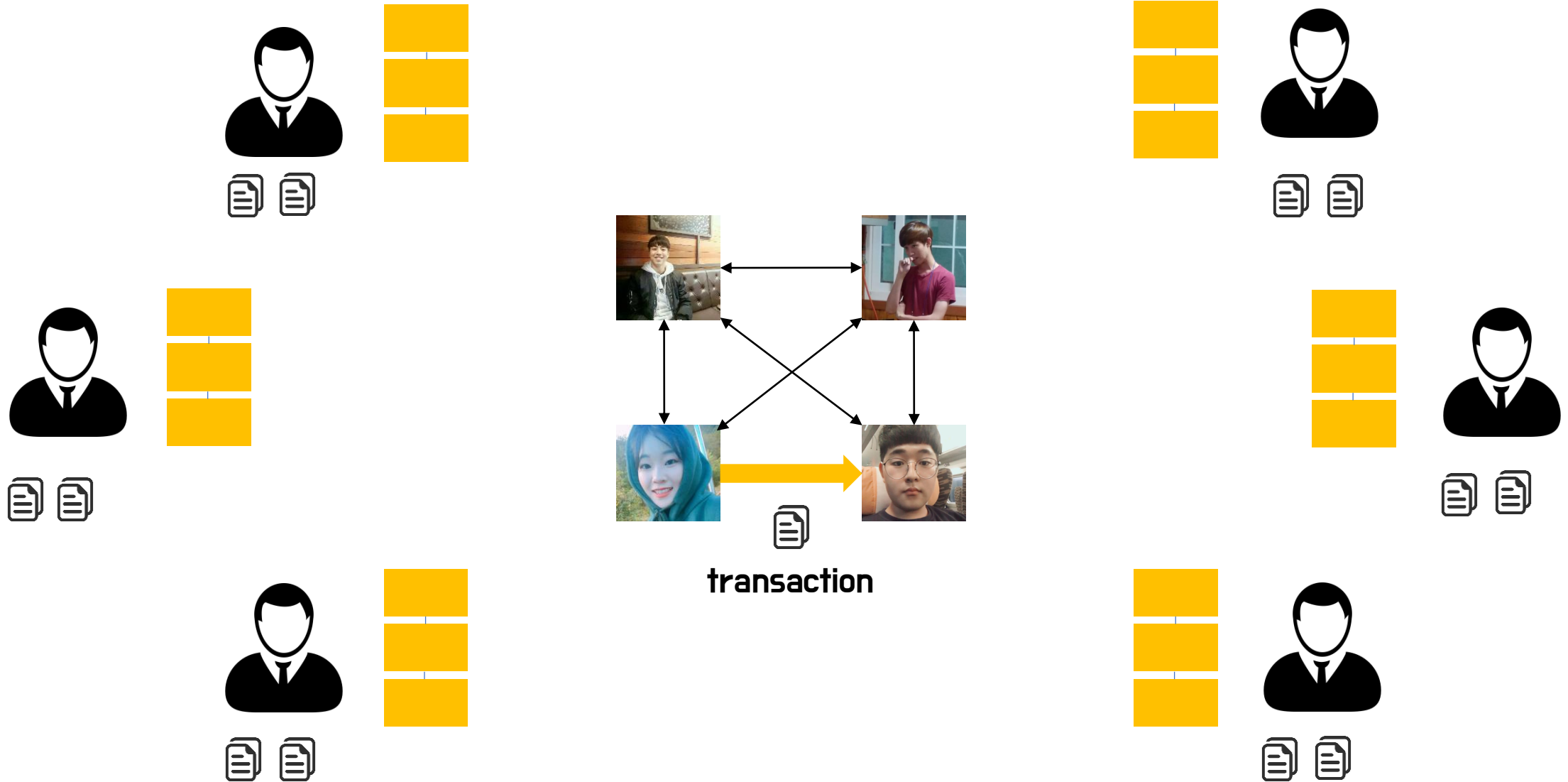
비트코인과 블록체인



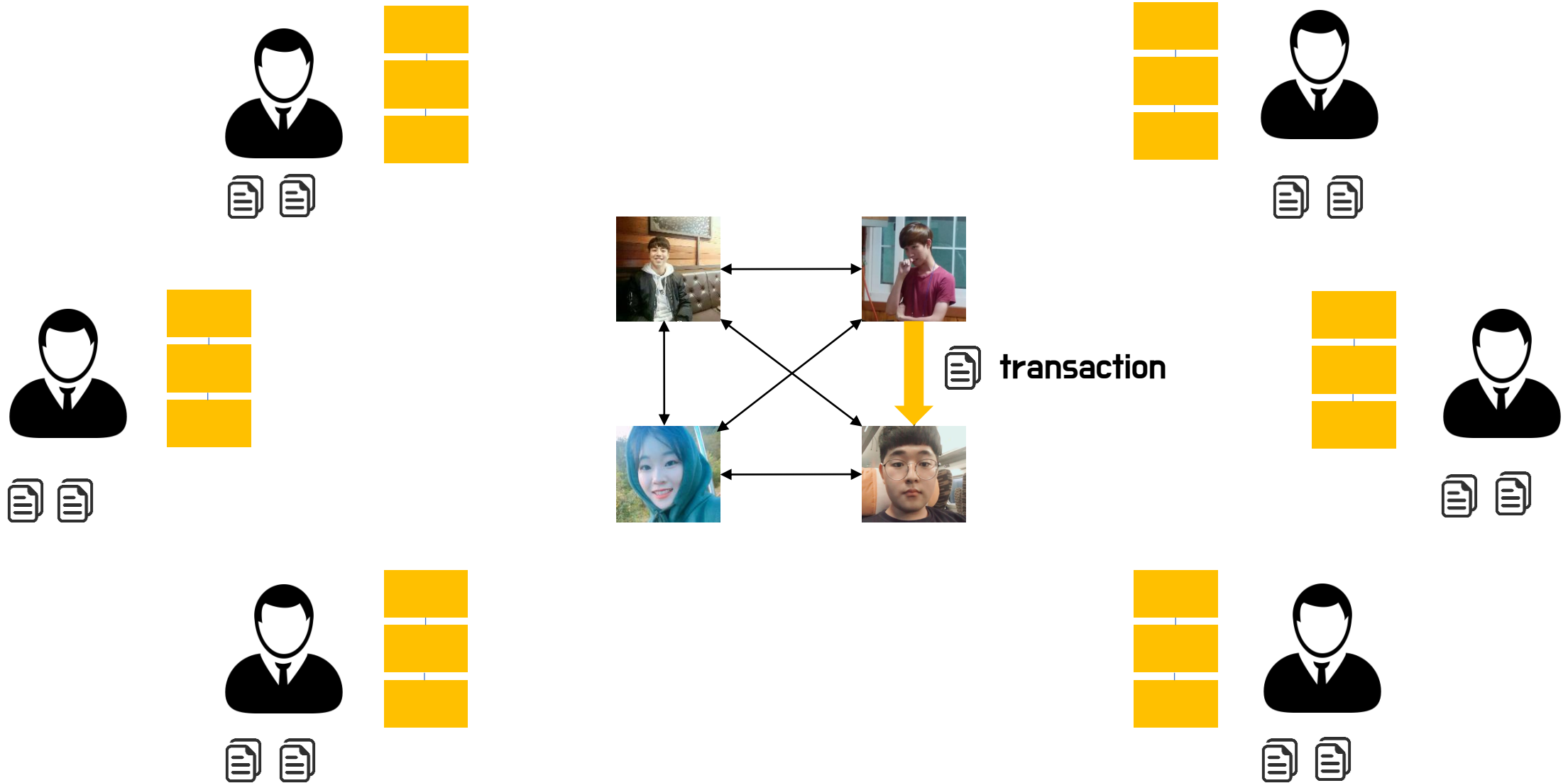
비트코인과 블록체인



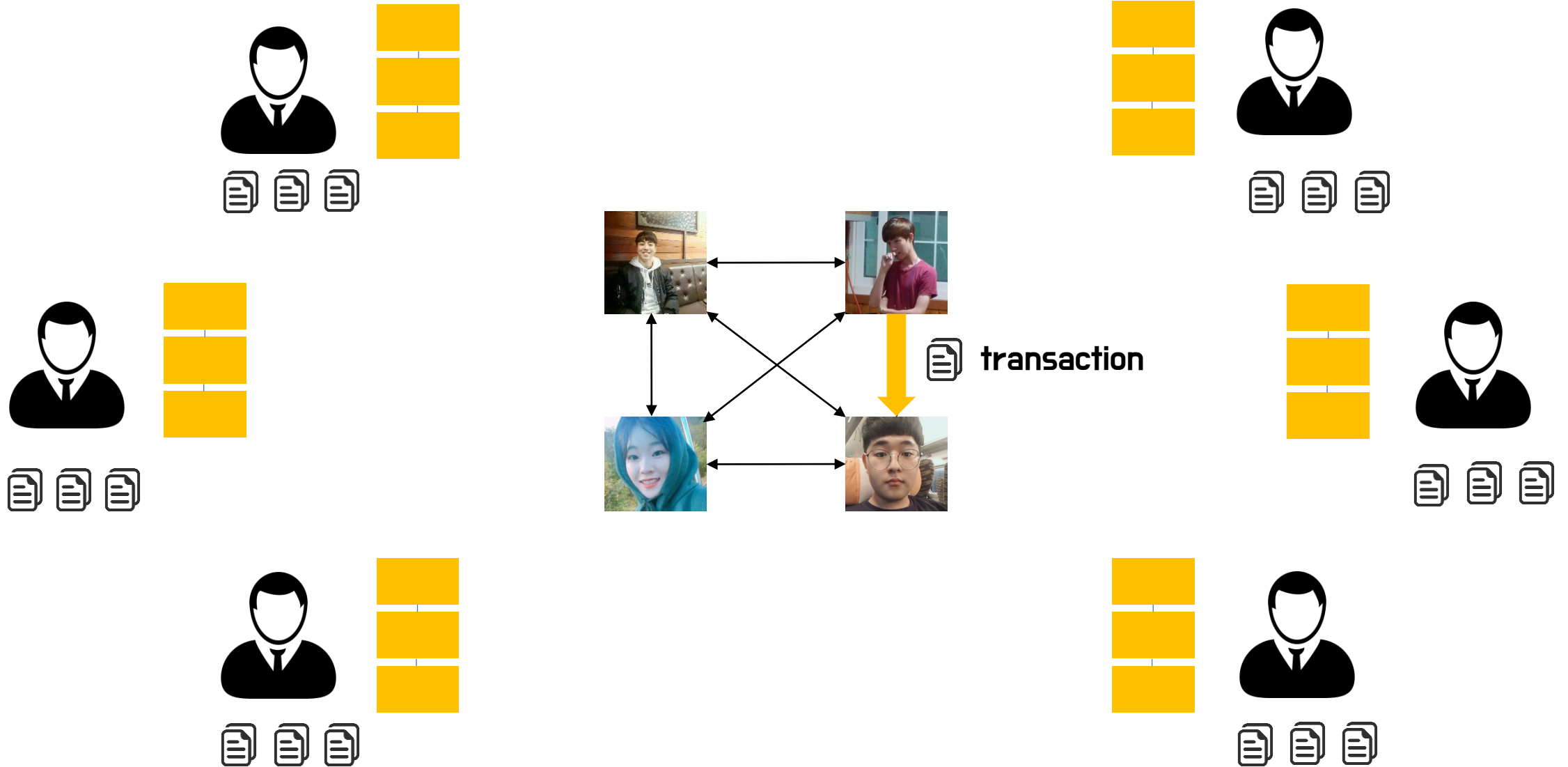
비트코인과 블록체인



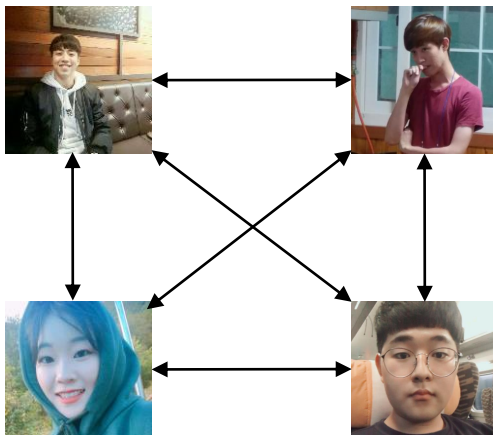
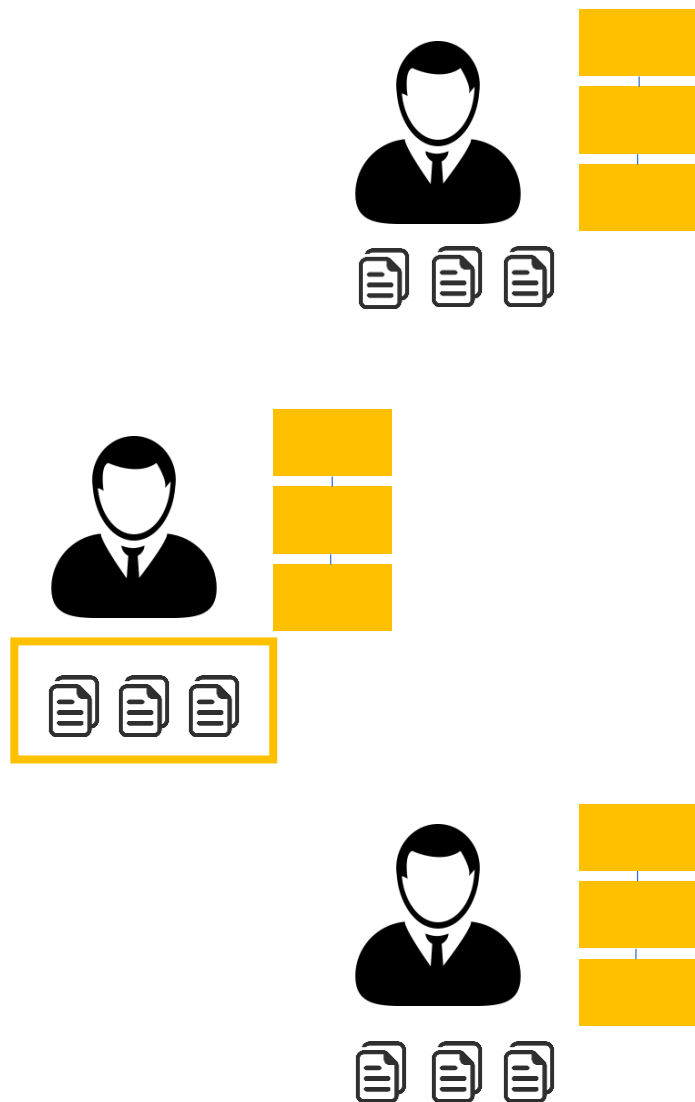
비트코인과 블록체인



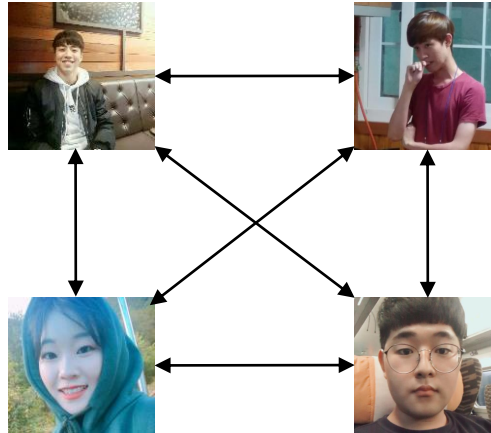
비트코인과 블록체인



비트코인과 블록체인



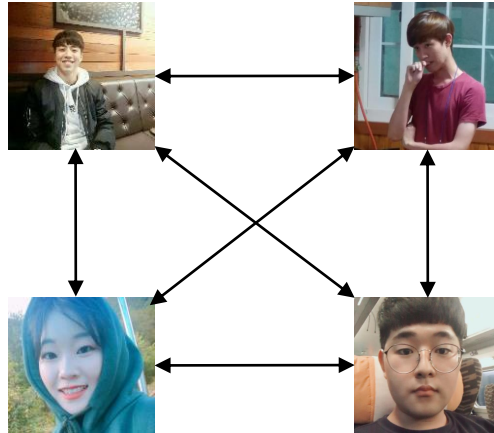
비트코인과 블록체인



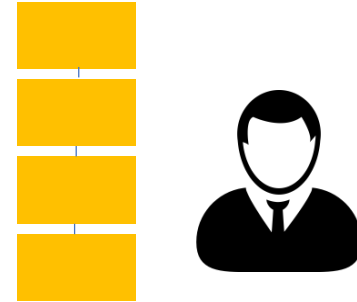
 최초로 블록 생성 성공!



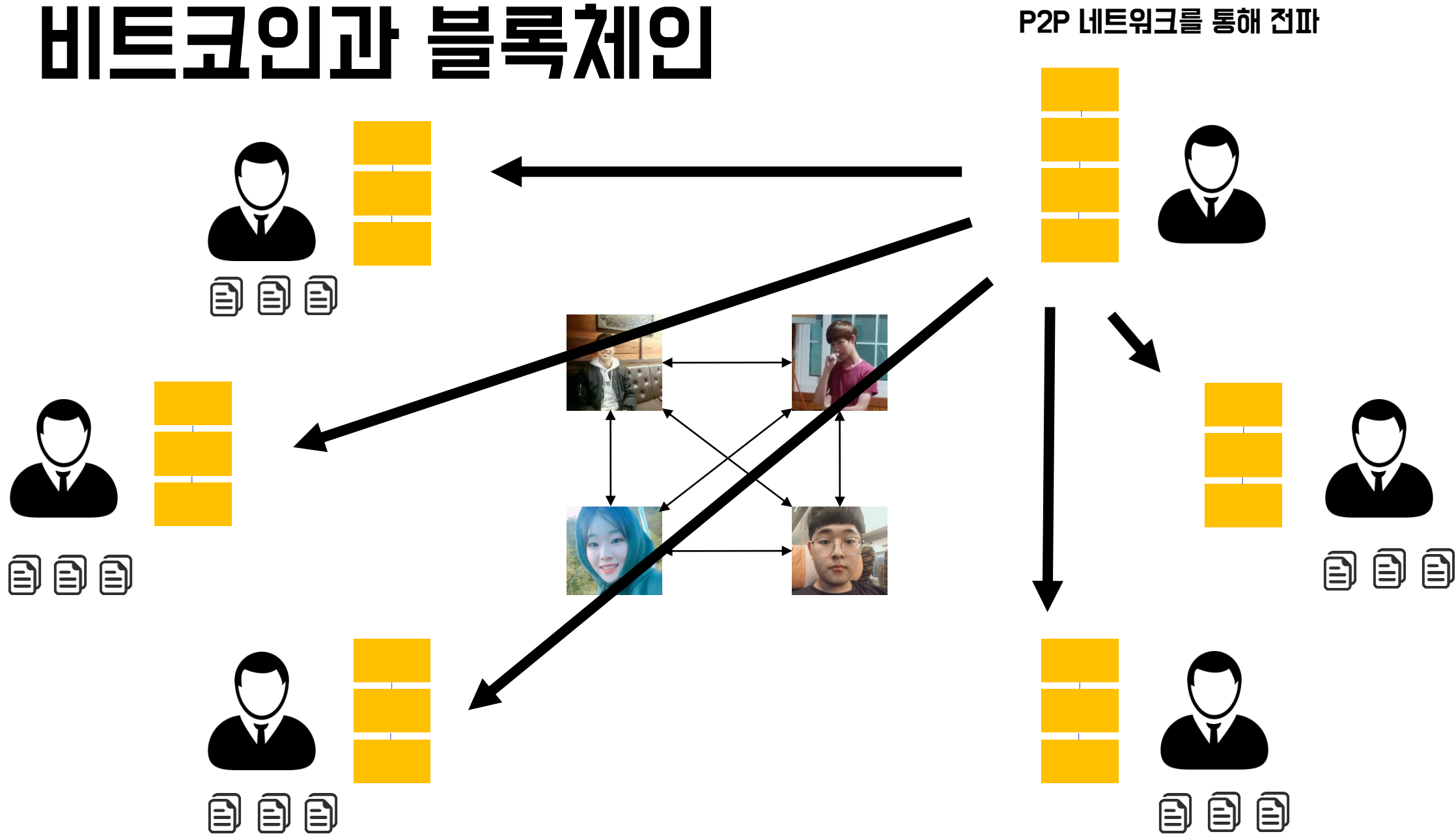
비트코인과 블록체인



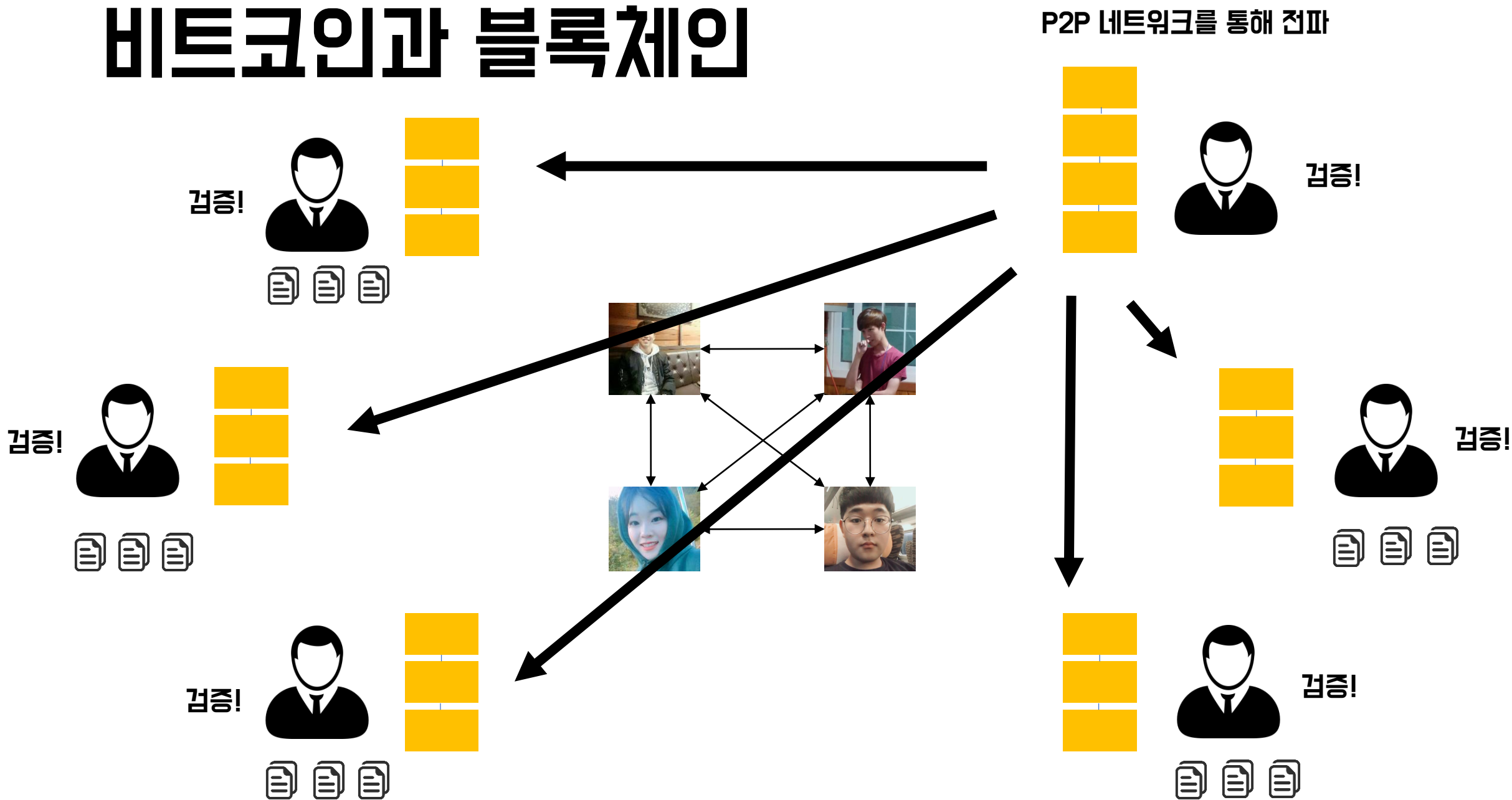
블록체인에 블록 추가!



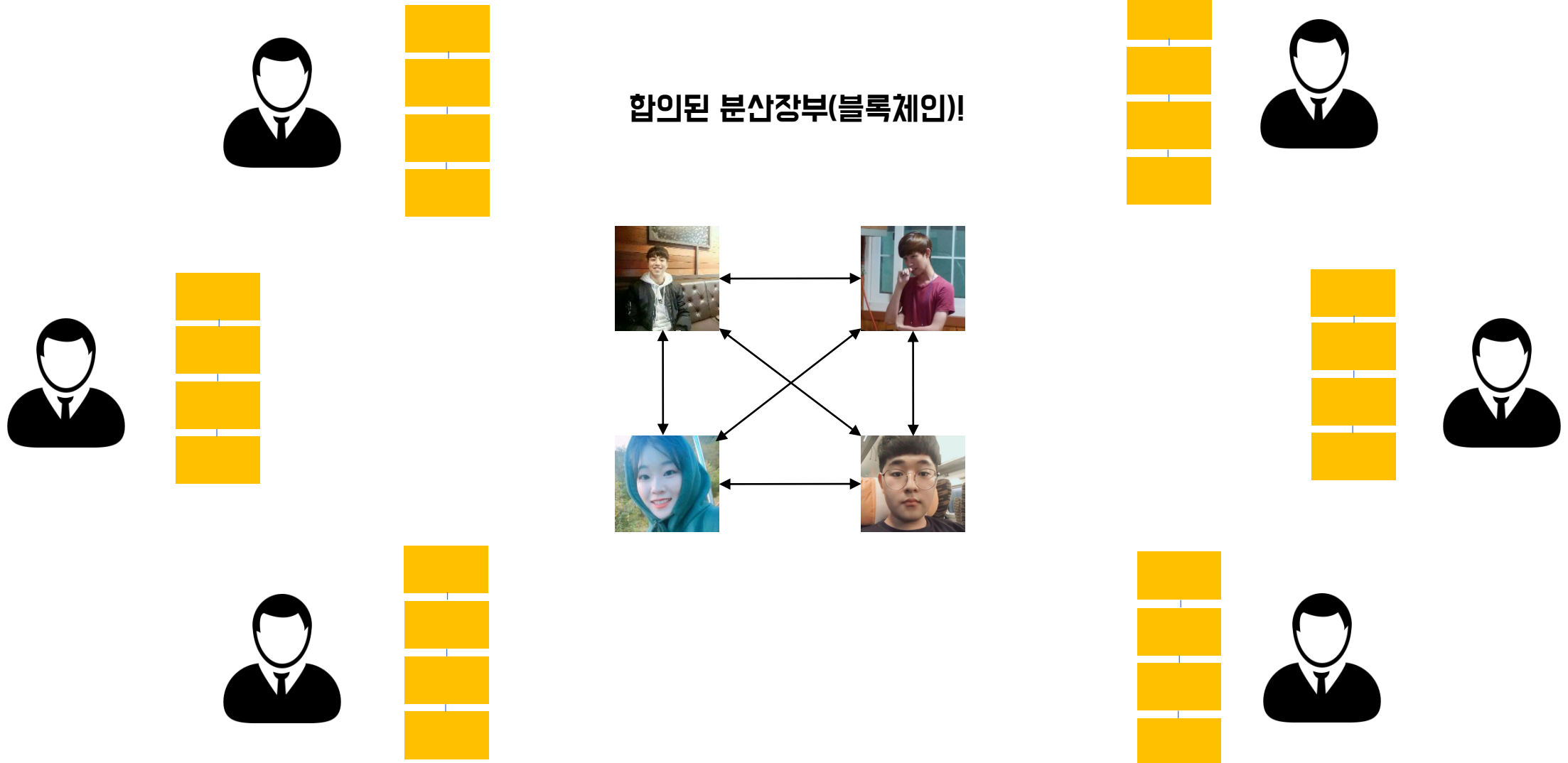
비트코인과 블록체인



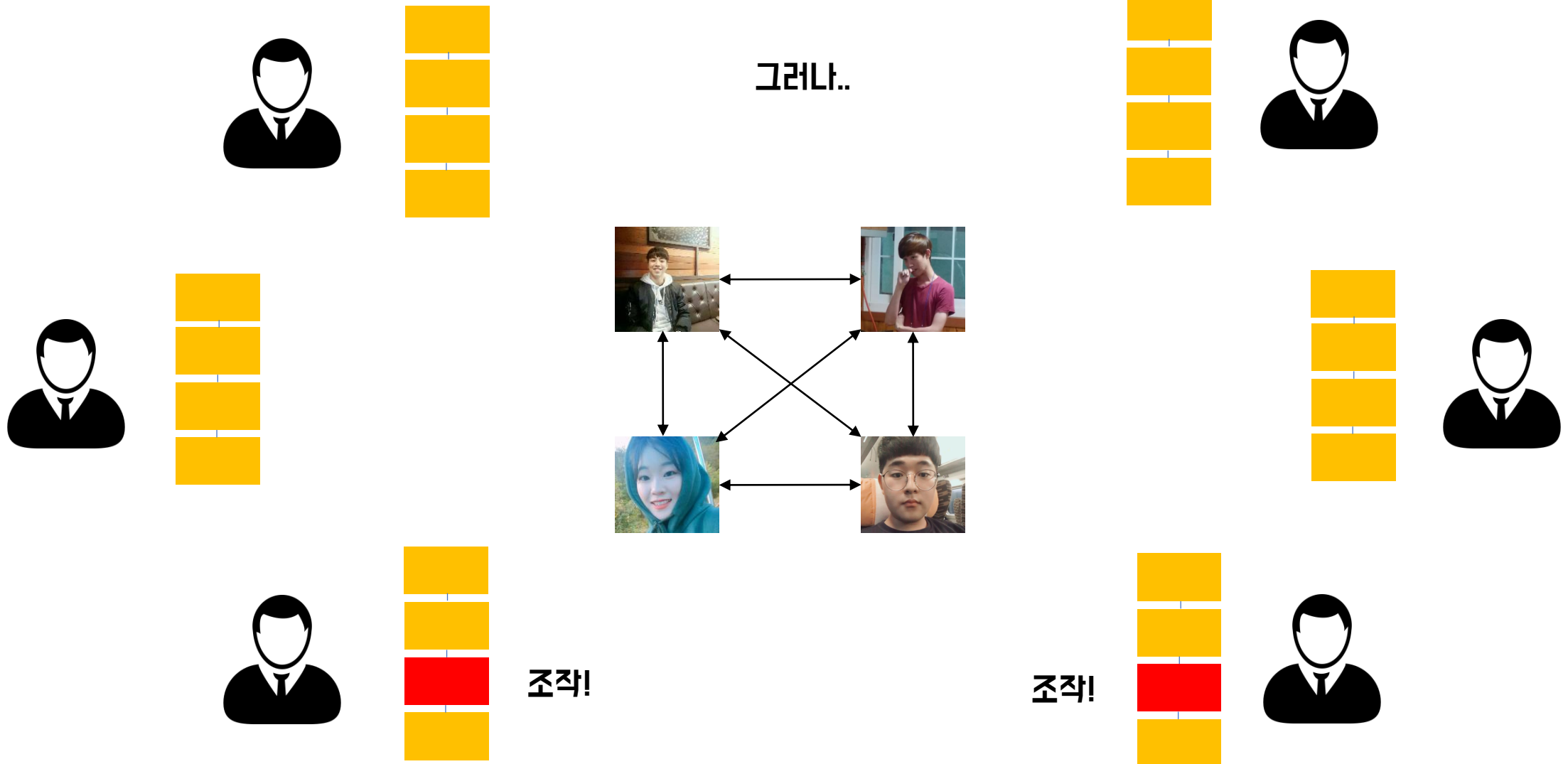
비트코인과 블록체인



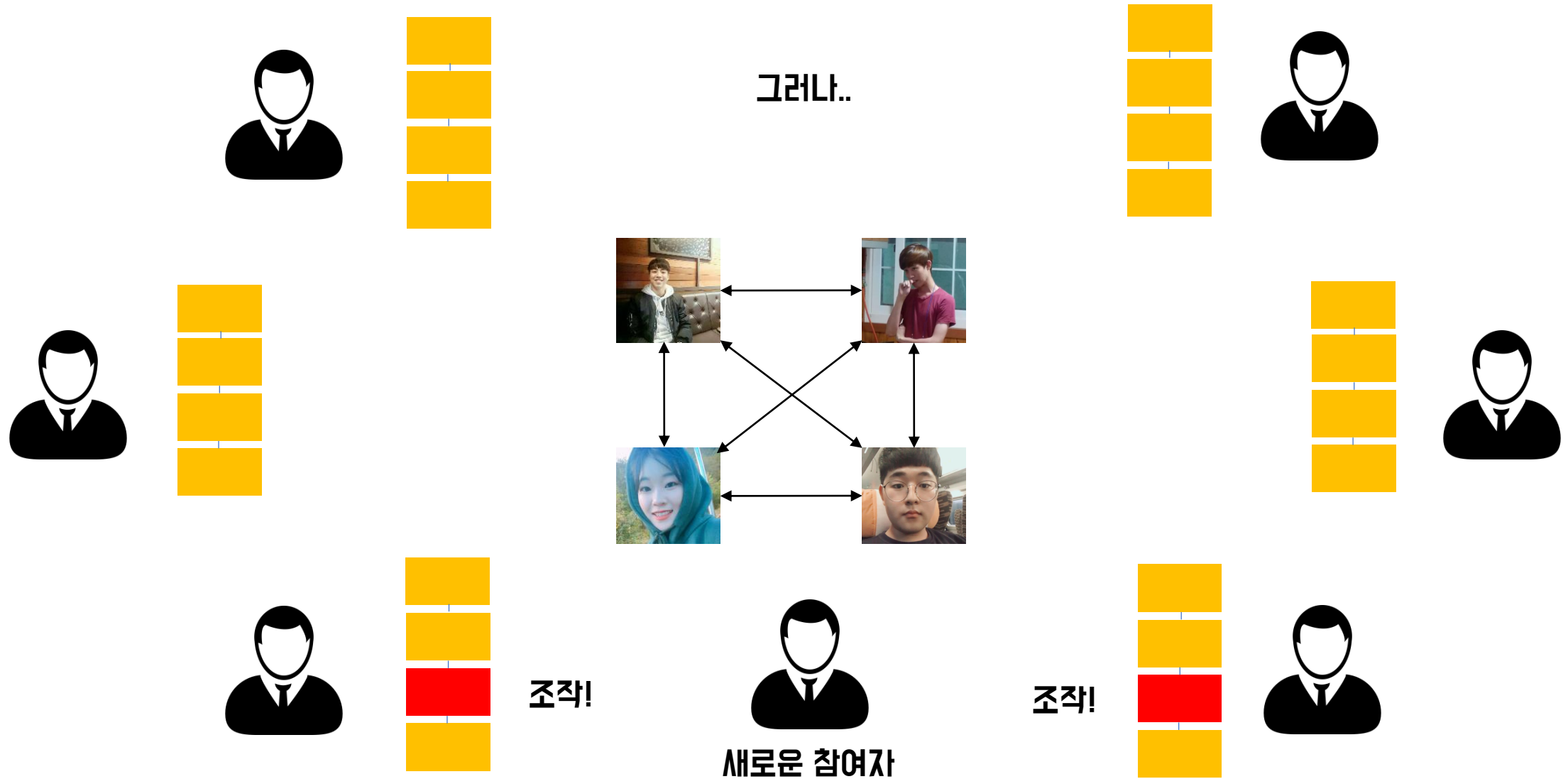
비트코인과 블록체인



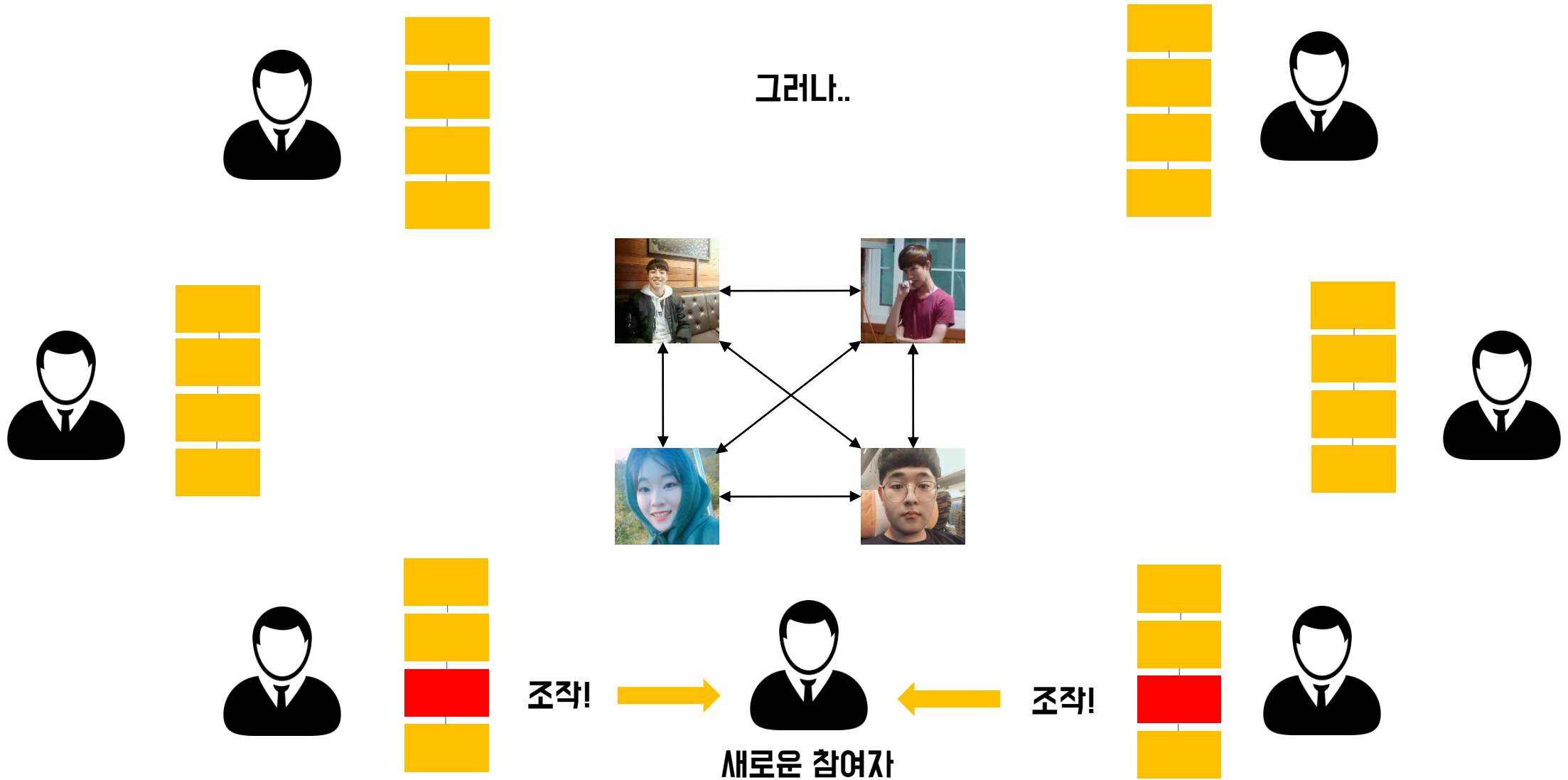
비트코인과 블록체인



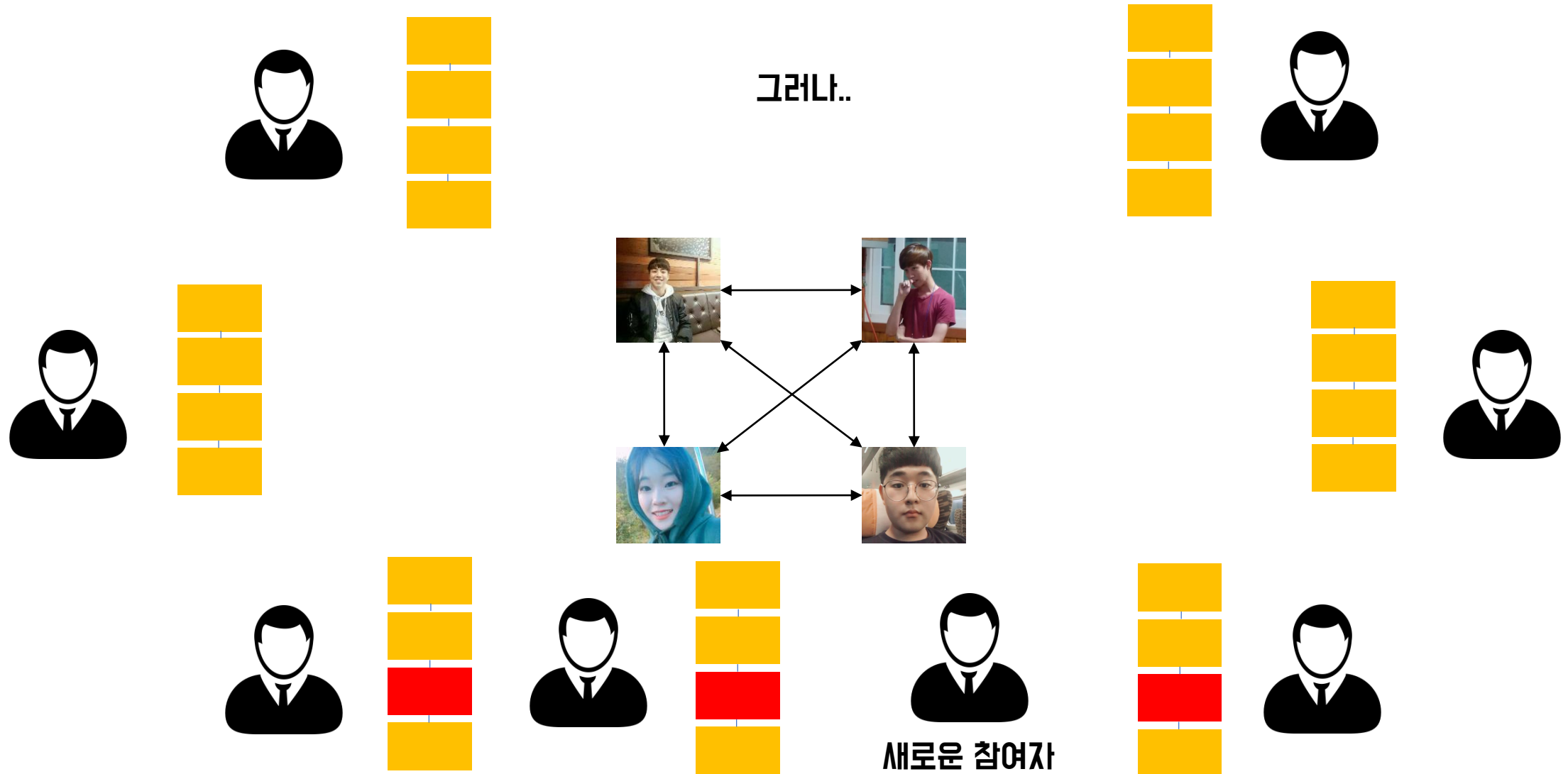
비트코인과 블록체인



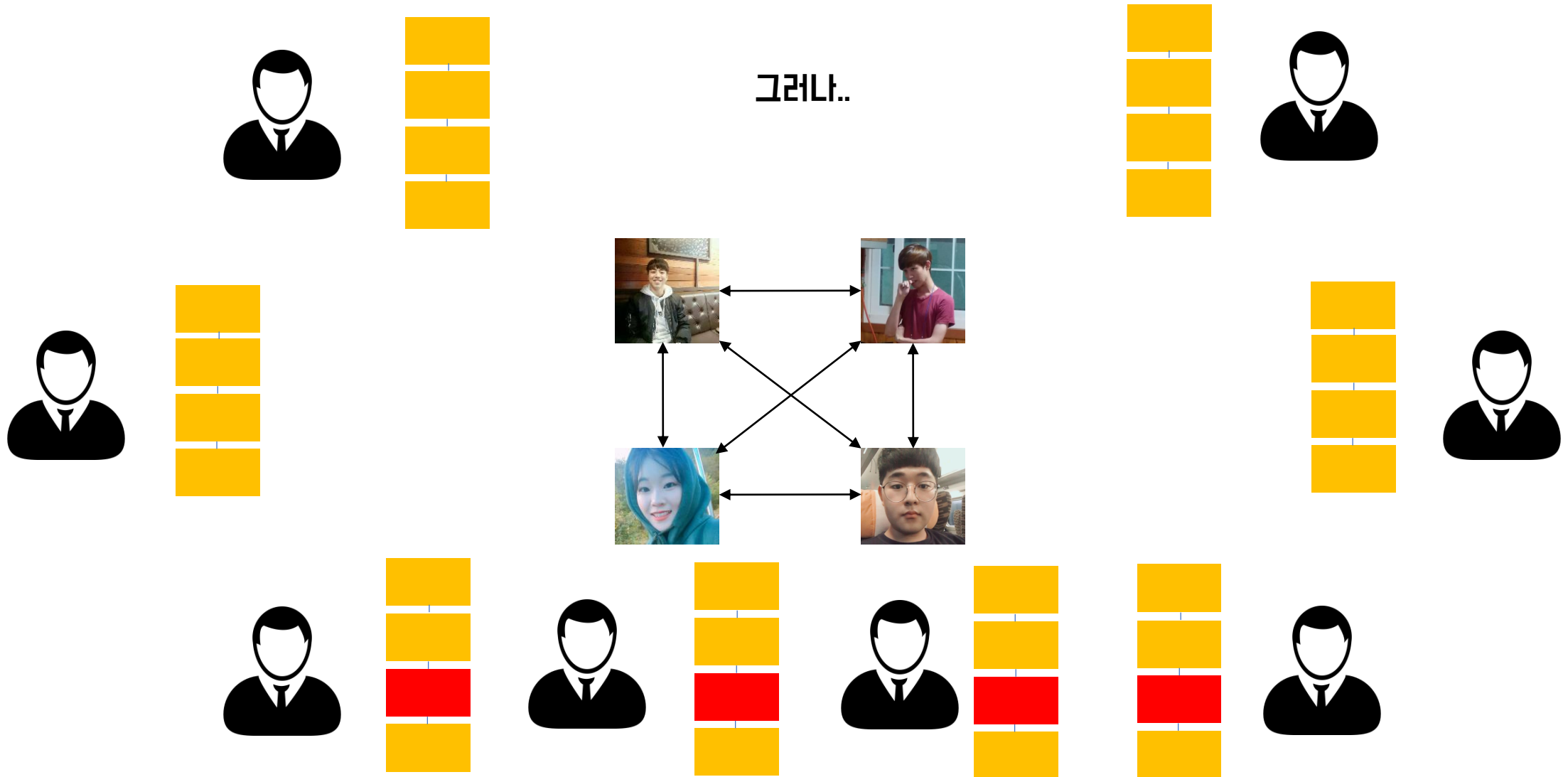
비트코인과 블록체인



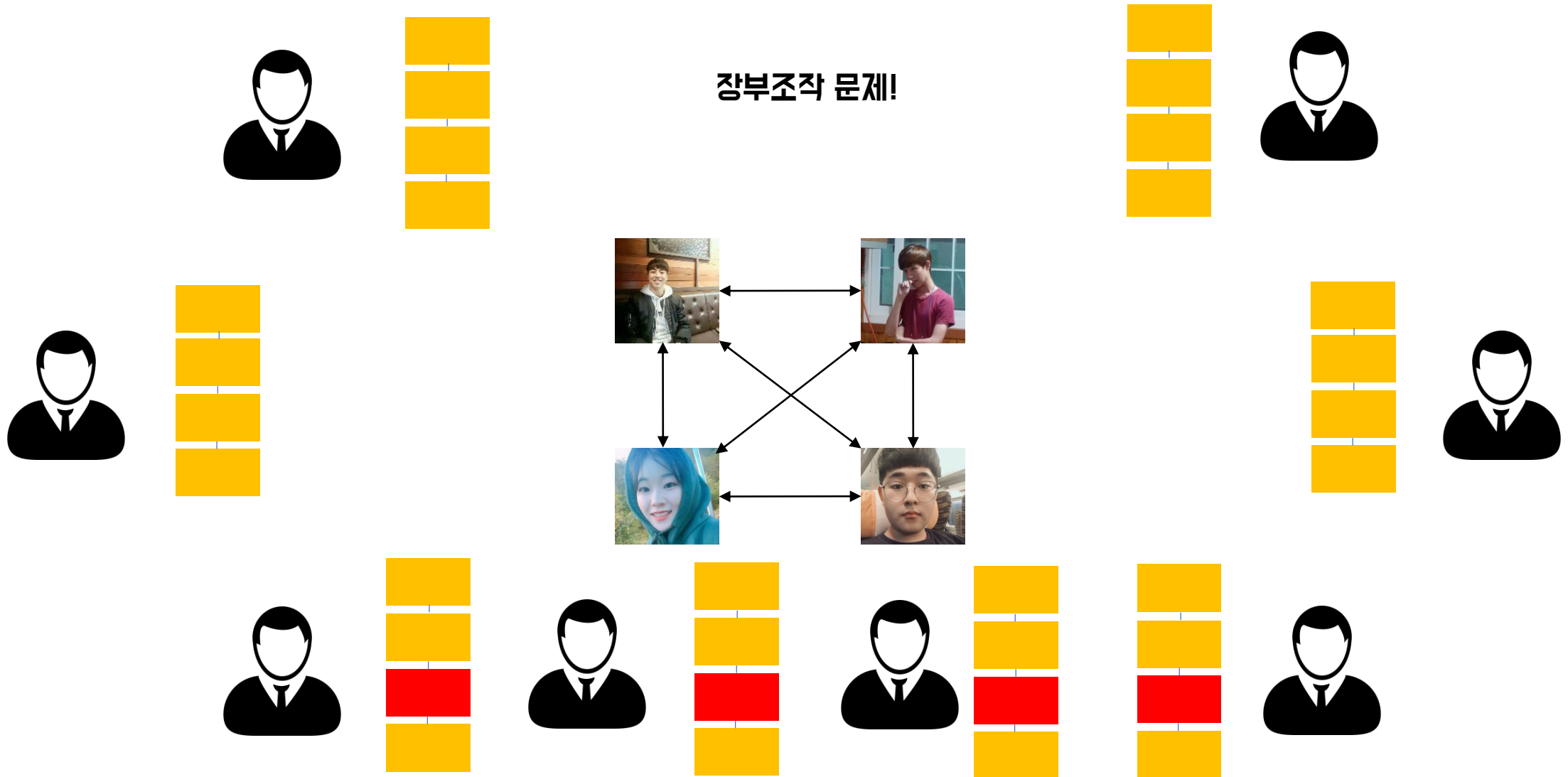
비트코인과 블록체인



비트코인과 블록체인



비트코인과 블록체인



비트코인의 거래유효성 입증



Q. 어떻게 장부조작을 방지할 것인가?

가상화폐 ?

제3의 '중앙 기관'에 의존하지 않는 화폐
인터넷상에서 자유롭게 사용가능한 화폐

비트코인의 거래유효성 입증



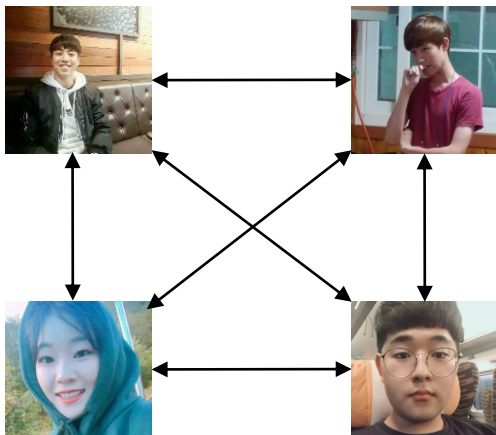
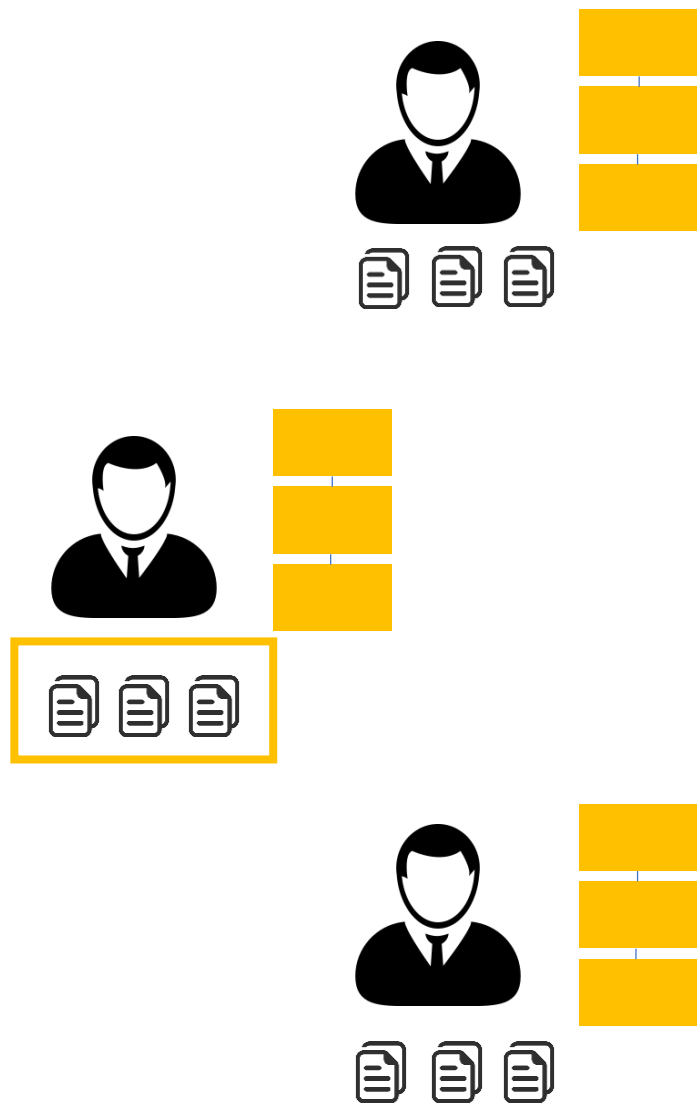
Q. 어떻게 장부조작을 방지할 것인가?

하나의 블록을 만드는 것 (장부를 작성하는 것)을 어렵게 만들자!

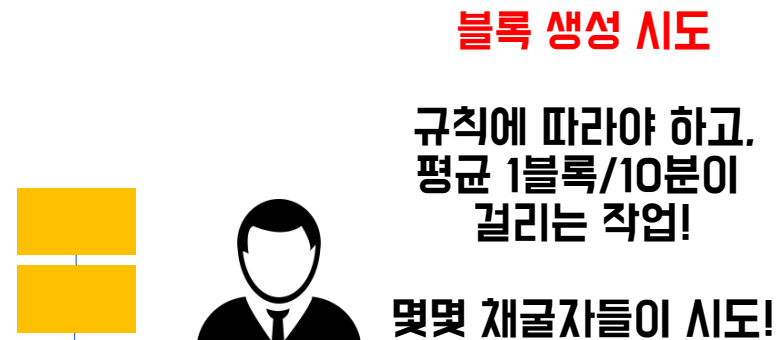
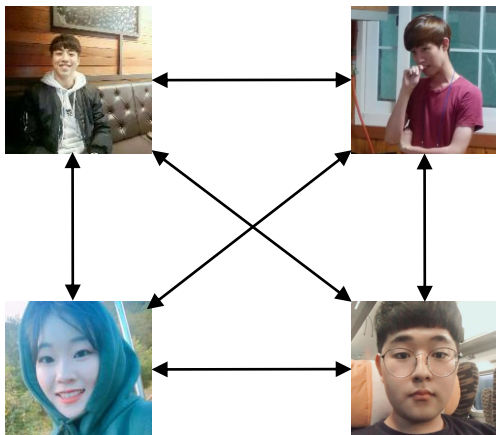
가상화폐 ?

제3의 '중앙 기관'에 의존하지 않는 화폐
인터넷상에서 자유롭게 사용가능한 화폐

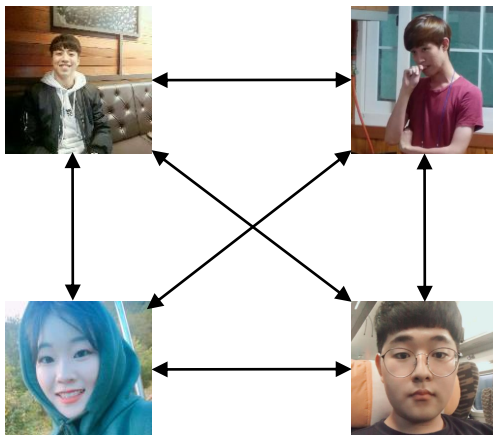
비트코인과 블록체인



비트코인과 블록체인



비트코인과 블록체인



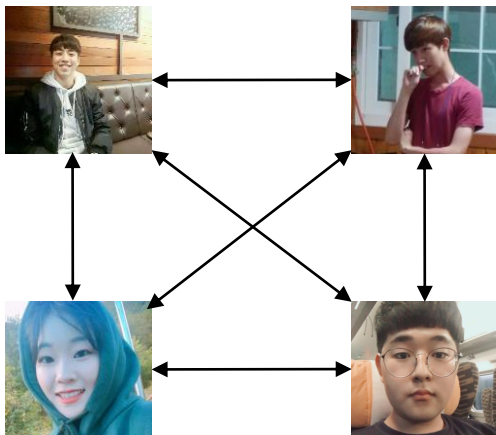
블록 생성 시도

규칙에 따라야 하고,
평균 1블록/10분이
걸리는 작업!

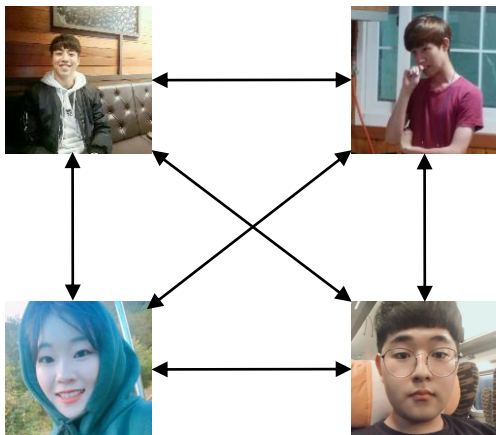
채굴자가 5000명?



비트코인과 블록체인



비트코인과 블록체인

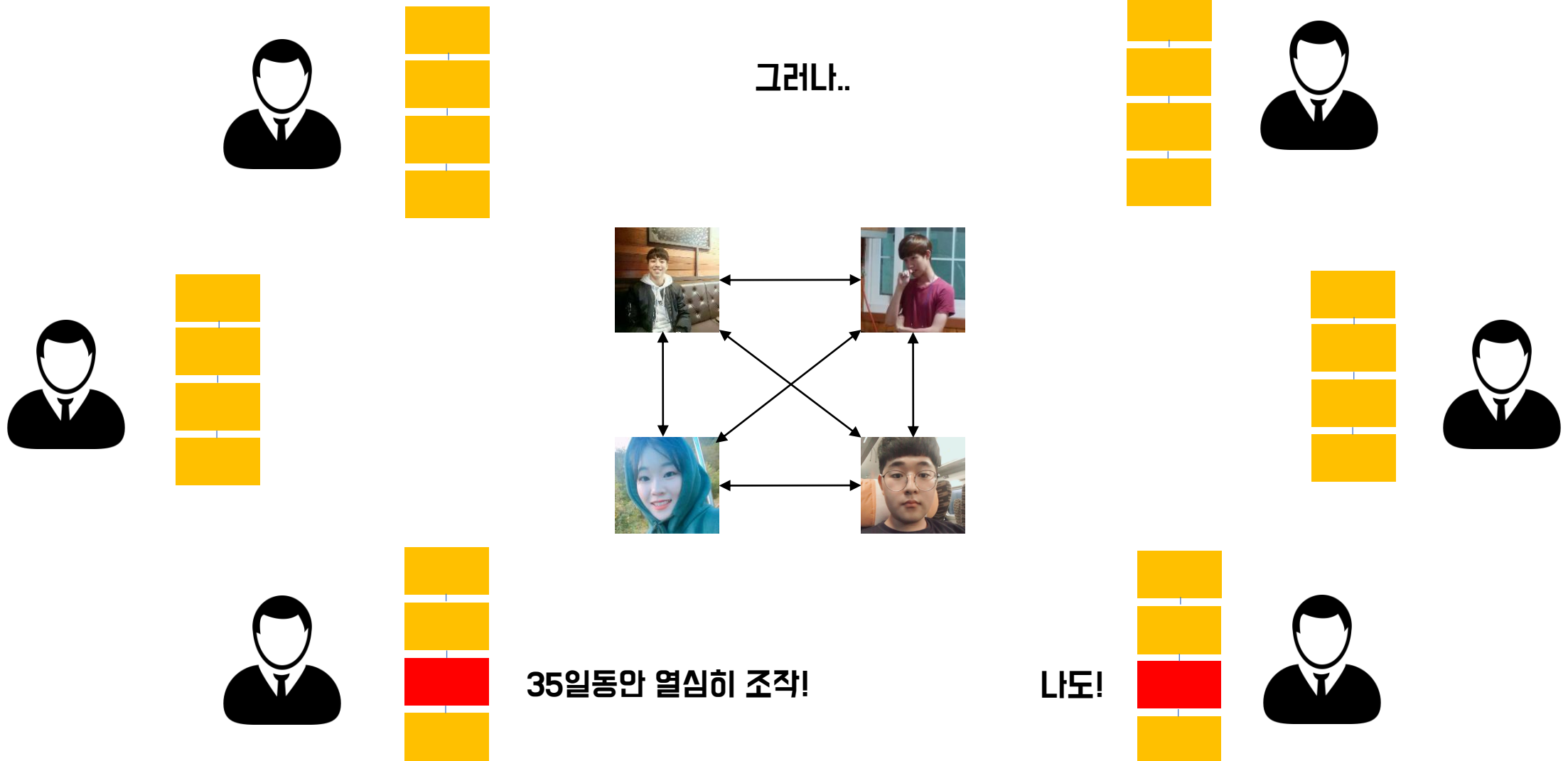


블록 생성 시도
규칙에 따라야 하고,
평균 1블록/10분이
걸리는 **어려운** 작업!

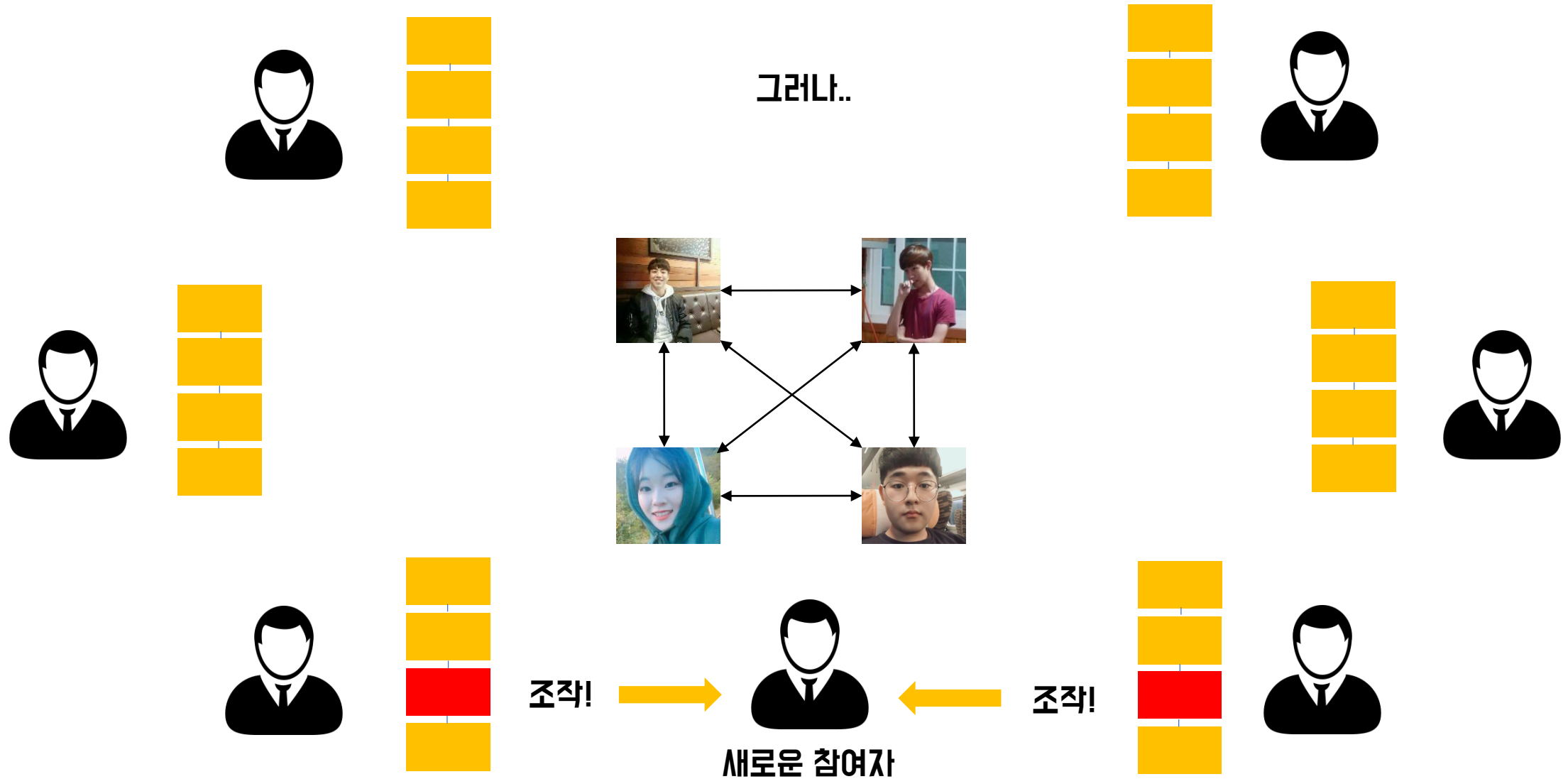
35일짜리 작업!



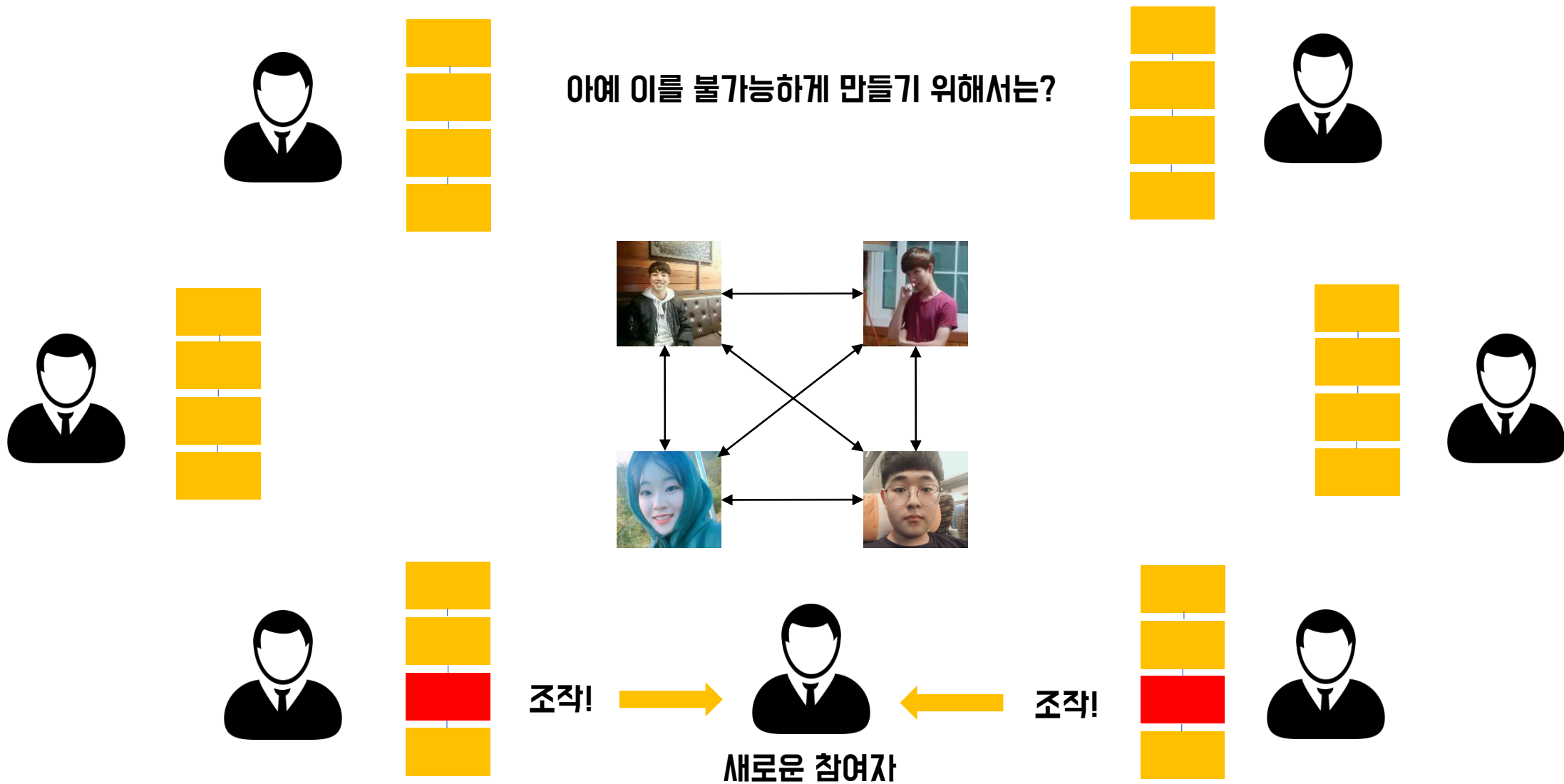
비트코인과 블록체인



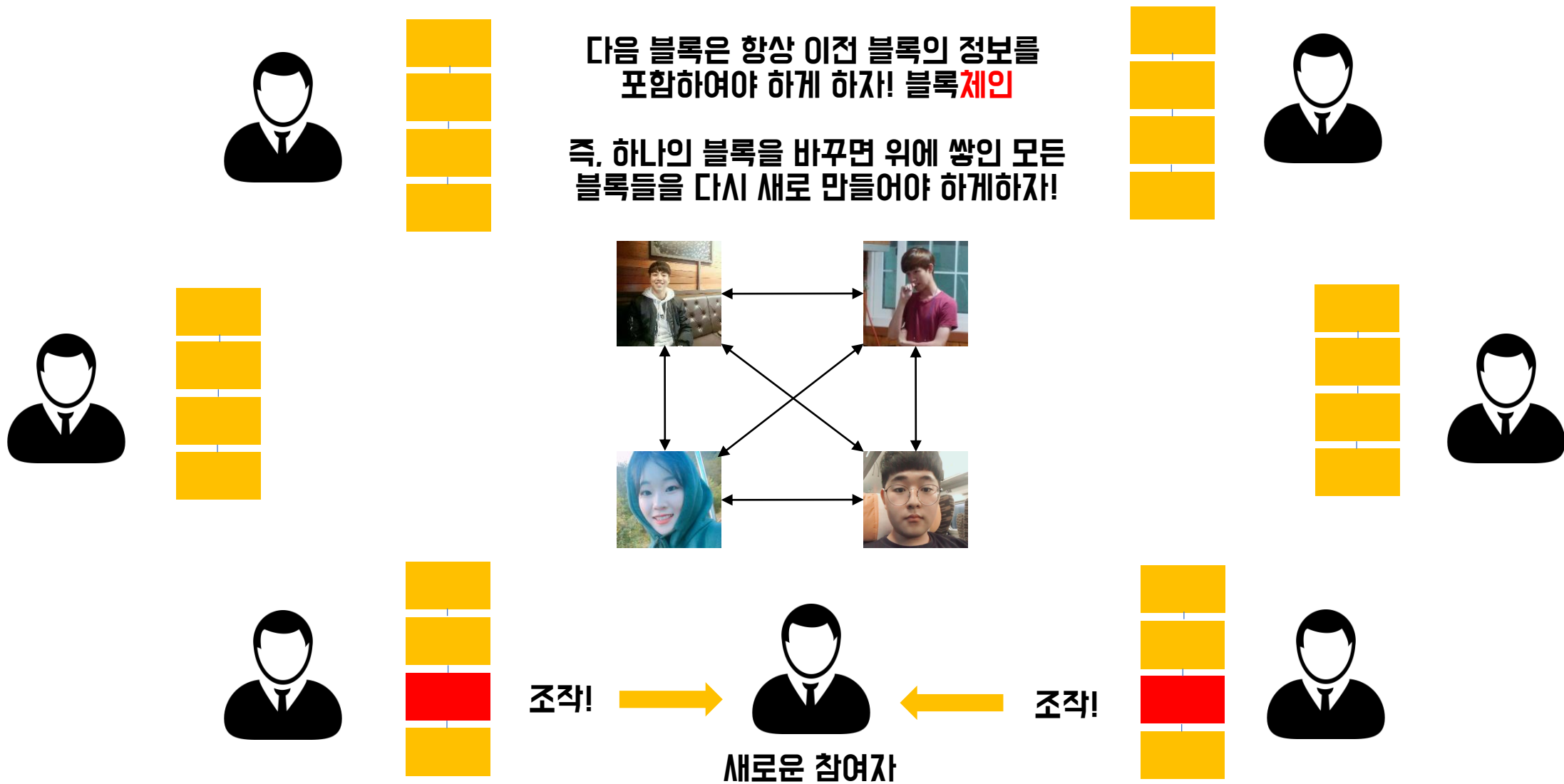
비트코인과 블록체인



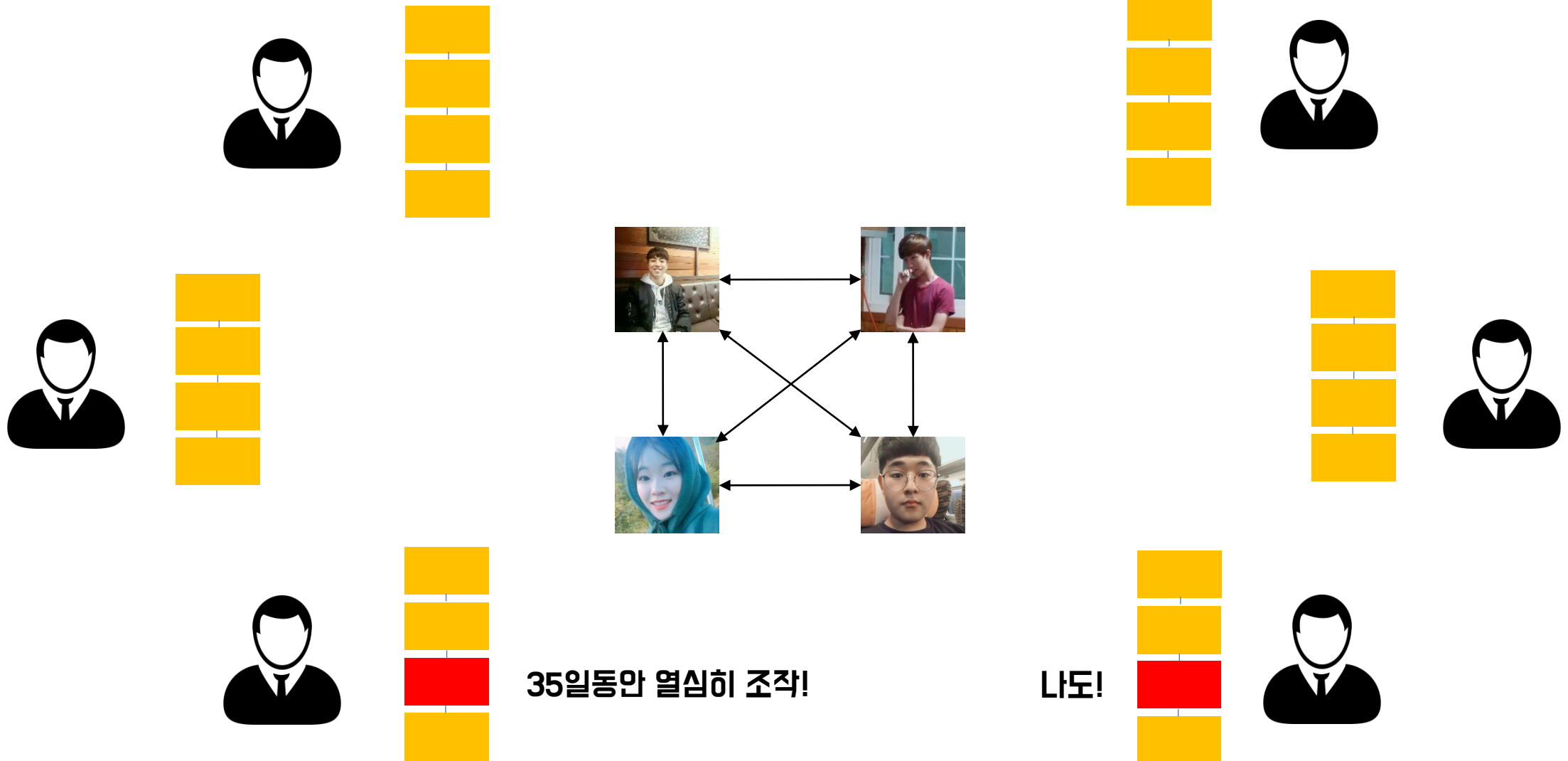
비트코인과 블록체인



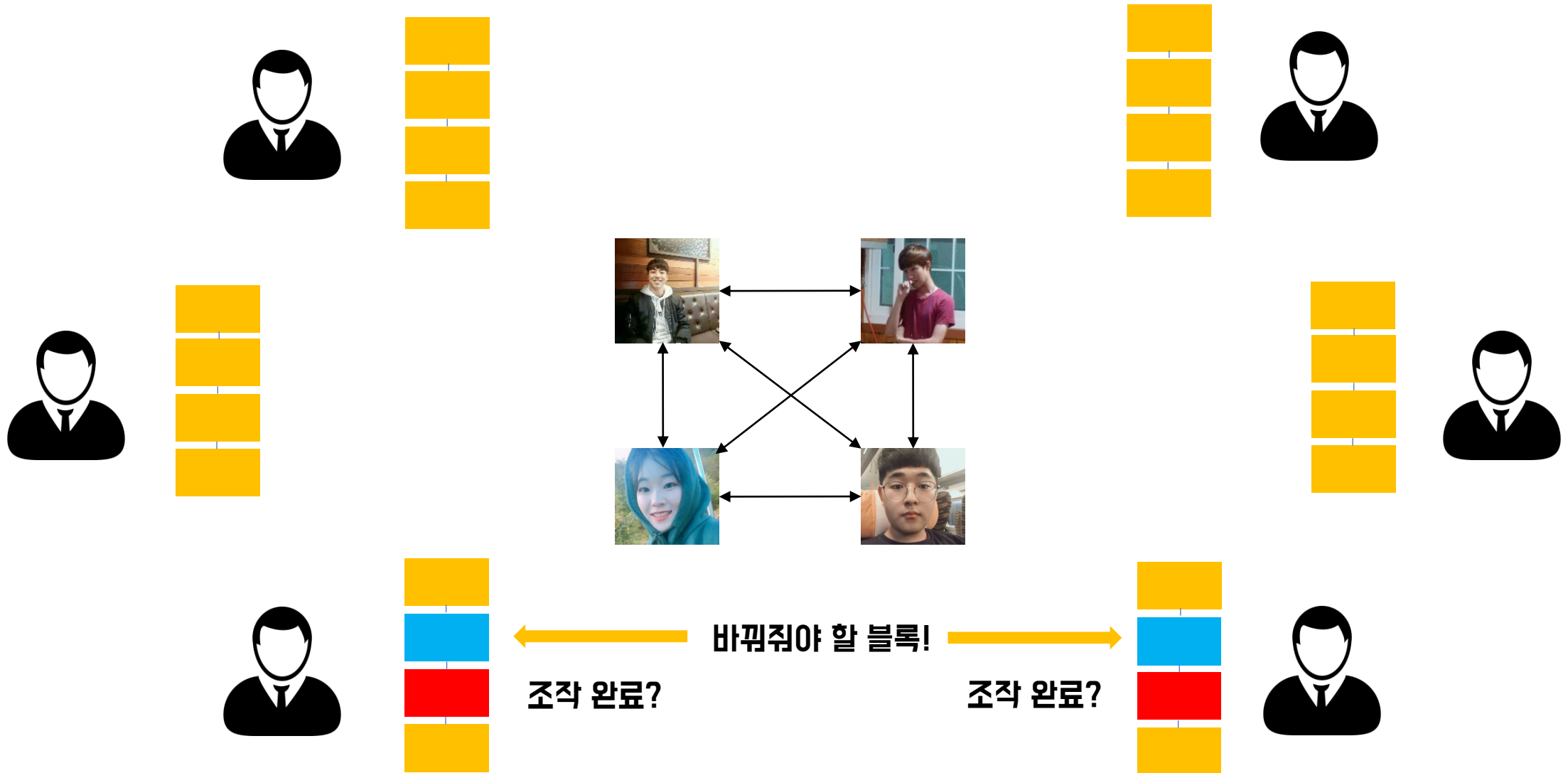
비트코인과 블록체인



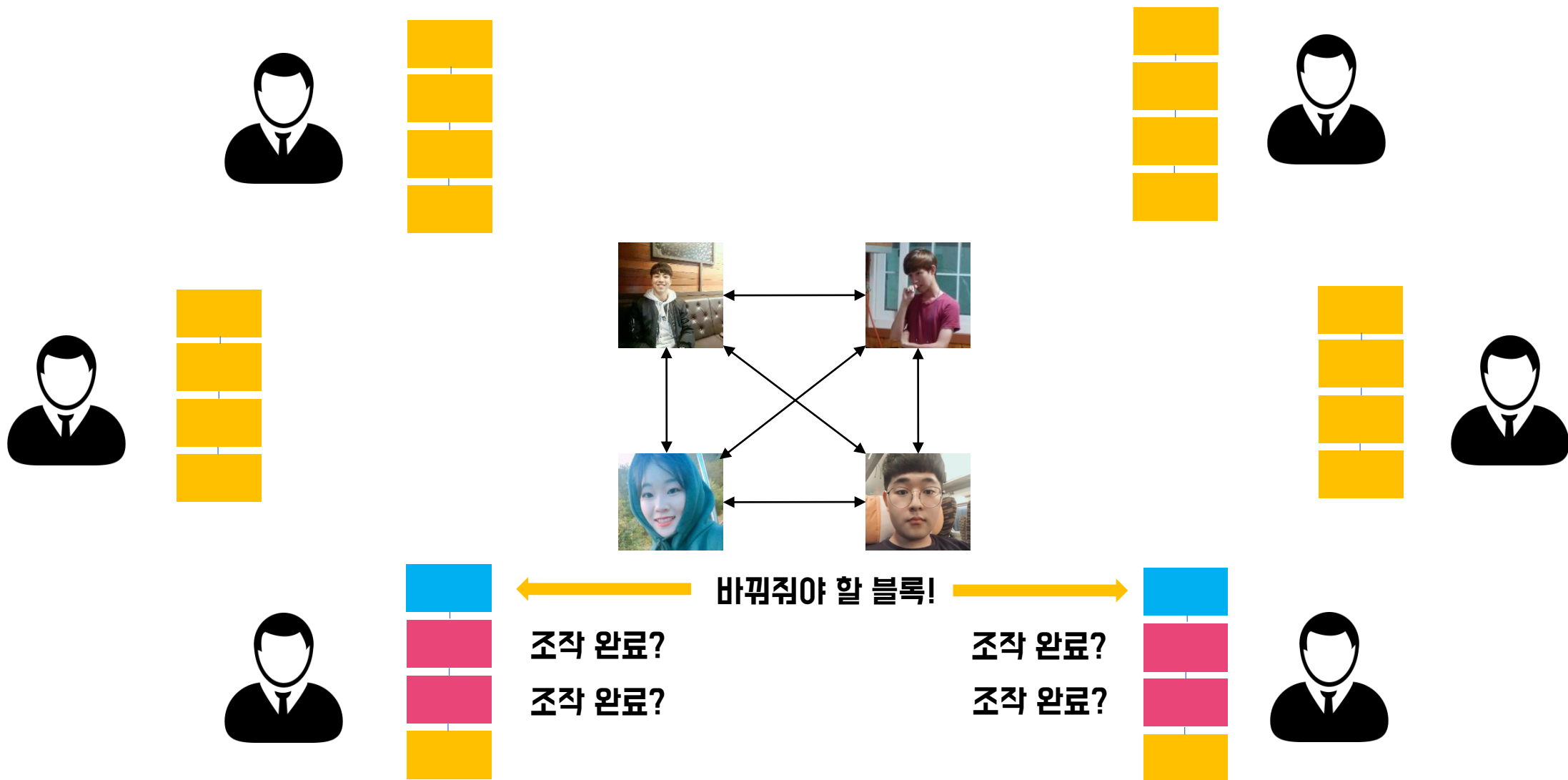
비트코인과 블록체인



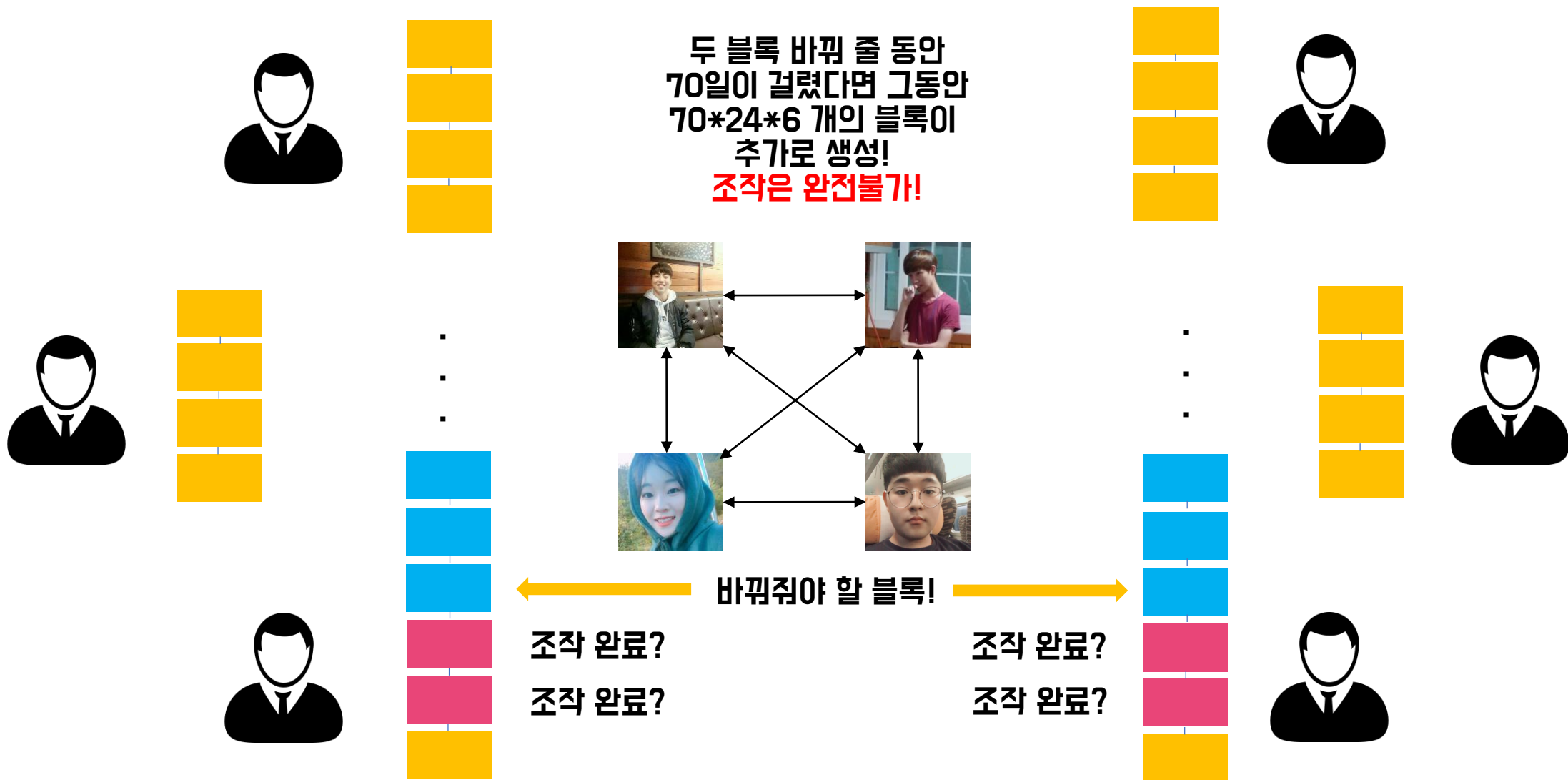
비트코인과 블록체인



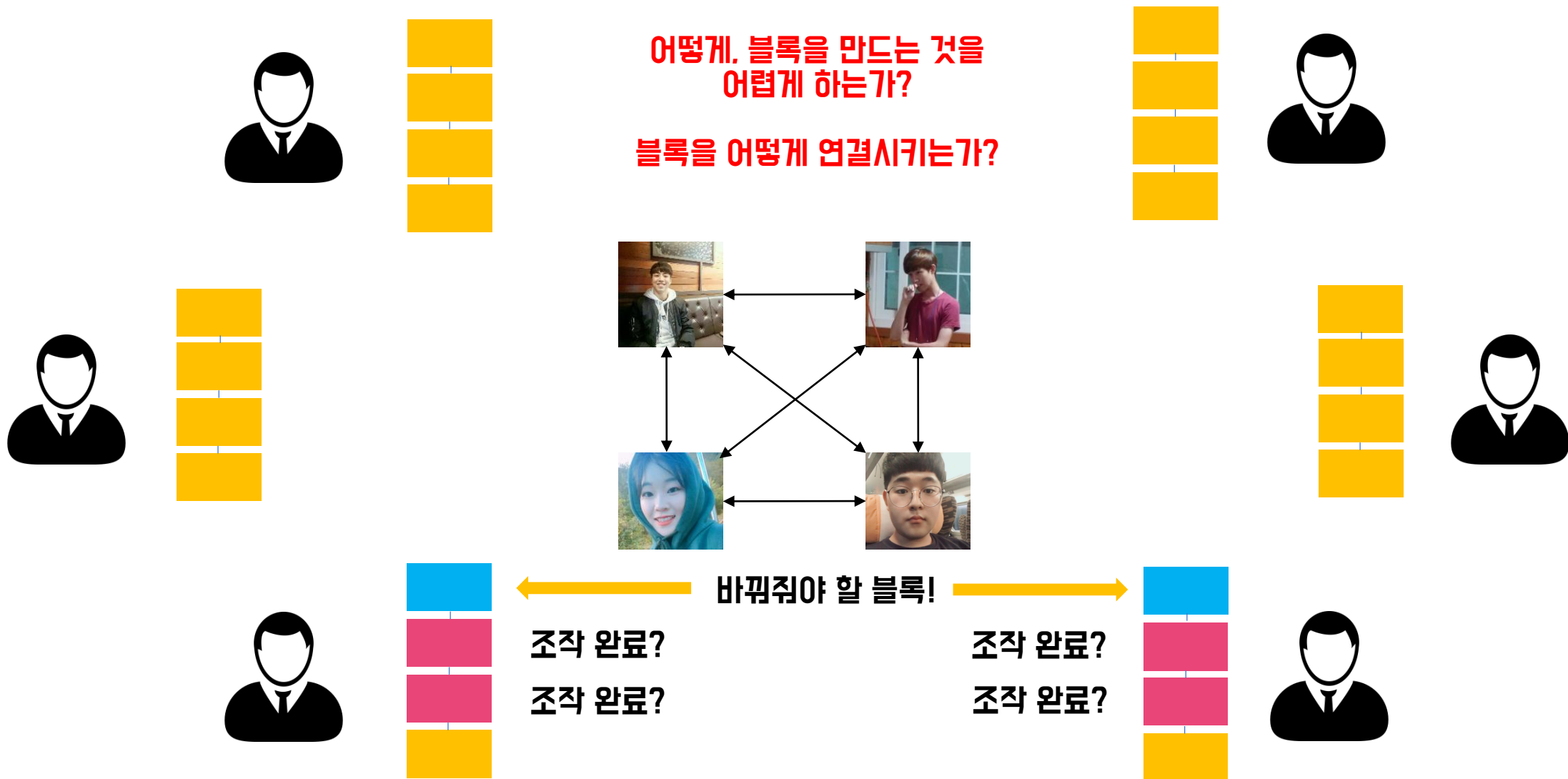
비트코인과 블록체인



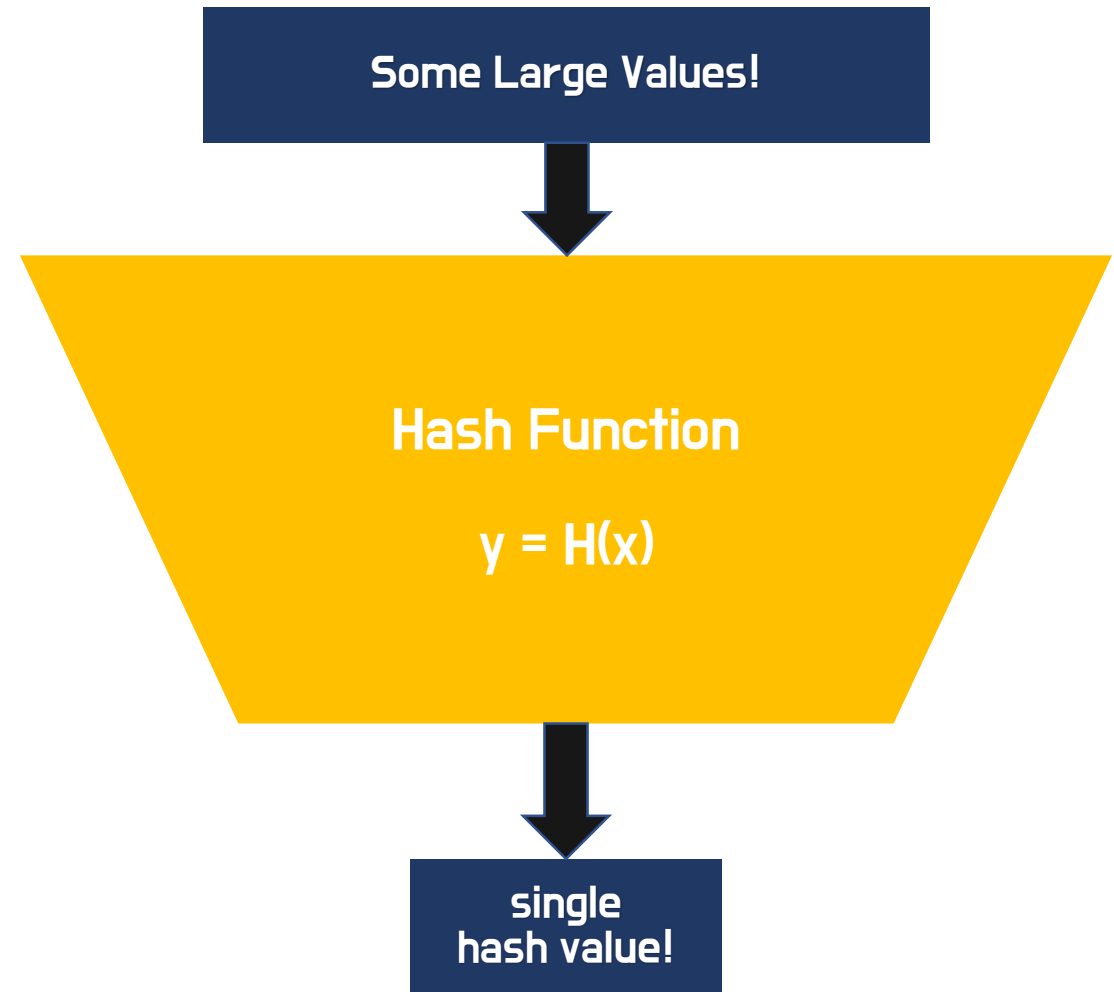
비트코인과 블록체인



비트코인과 블록체인



해쉬, 해쉬함수란?



블록체인 원리

From: 강재윤
TO: 김재호
Amount: 2,000,000 BTC

From: 박수현
TO: 강재윤
Amount: 1,000,000 BTC

From: 박수현
TO: 김재호
Amount: 3,000,000 BTC

개별거래기록

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000007ea...

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000006bc...

블록체인 원리

From: 강재윤
TO: 김재호
Amount: 2,000,000 BTC

From: 박수현
TO: 강재윤
Amount: 1,000,000 BTC

From: 박수현
TO: 김재호
Amount: 3,000,000 BTC

개별거래기록

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000007ea...

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

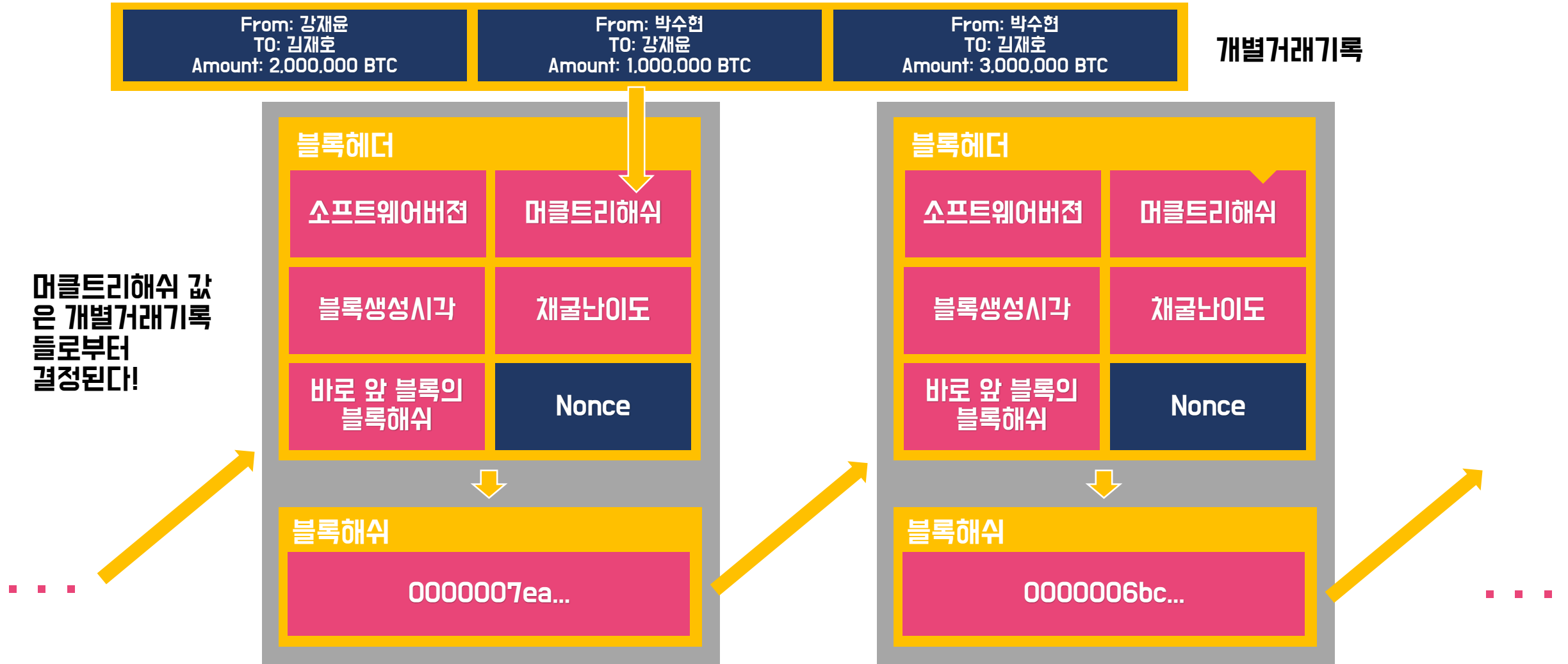
0000006bc...

블록해쉬 값은
블록헤더의
6개 값에 의해
결정된다!

...

...

블록체인 원리



블록체인 원리

From: 강재윤
TO: 김재호
Amount: 2,000,000 BTC

From: 박수현
TO: 강재윤
Amount: 1,000,000 BTC

From: 박수현
TO: 김재호
Amount: 3,000,000 BTC

개별거래기록

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000007ea...

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

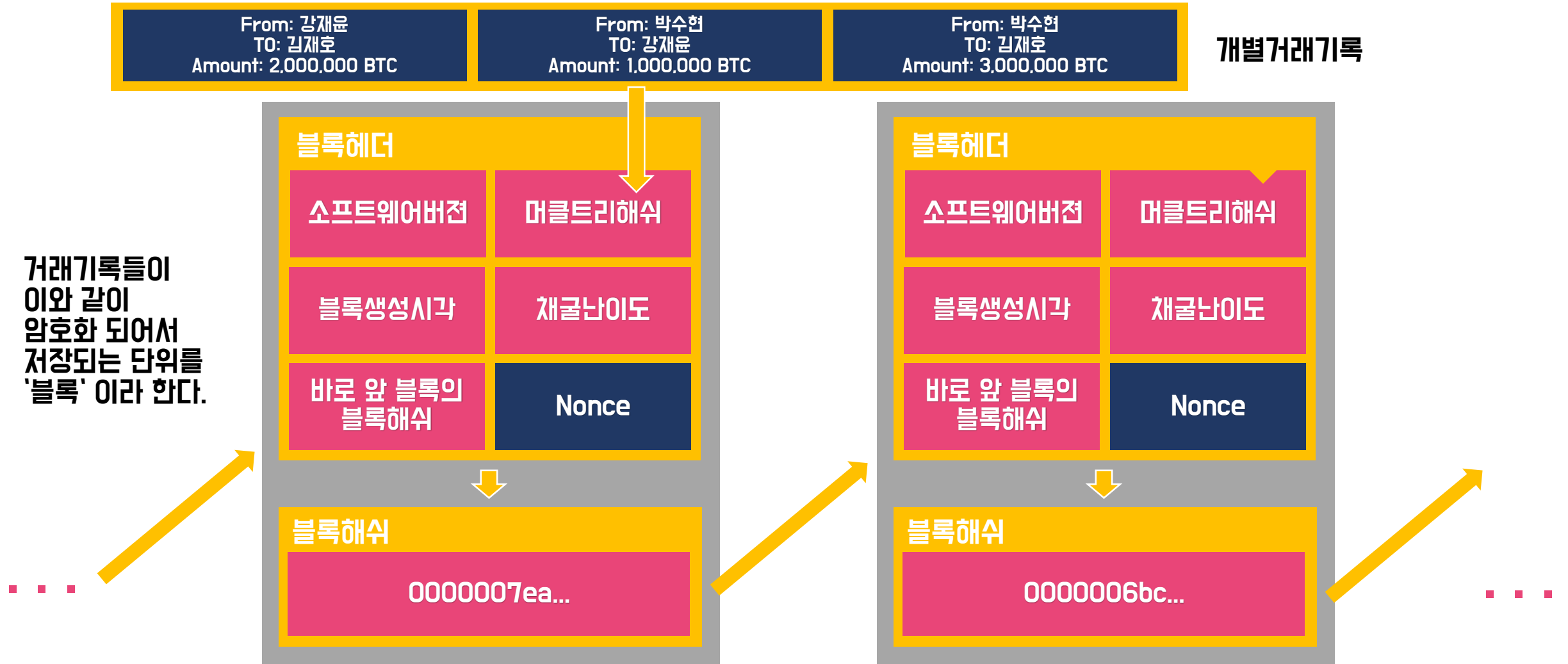
0000006bc...

즉, 거래기록을
모아서
블록해쉬 값을
계산할 수 있다!

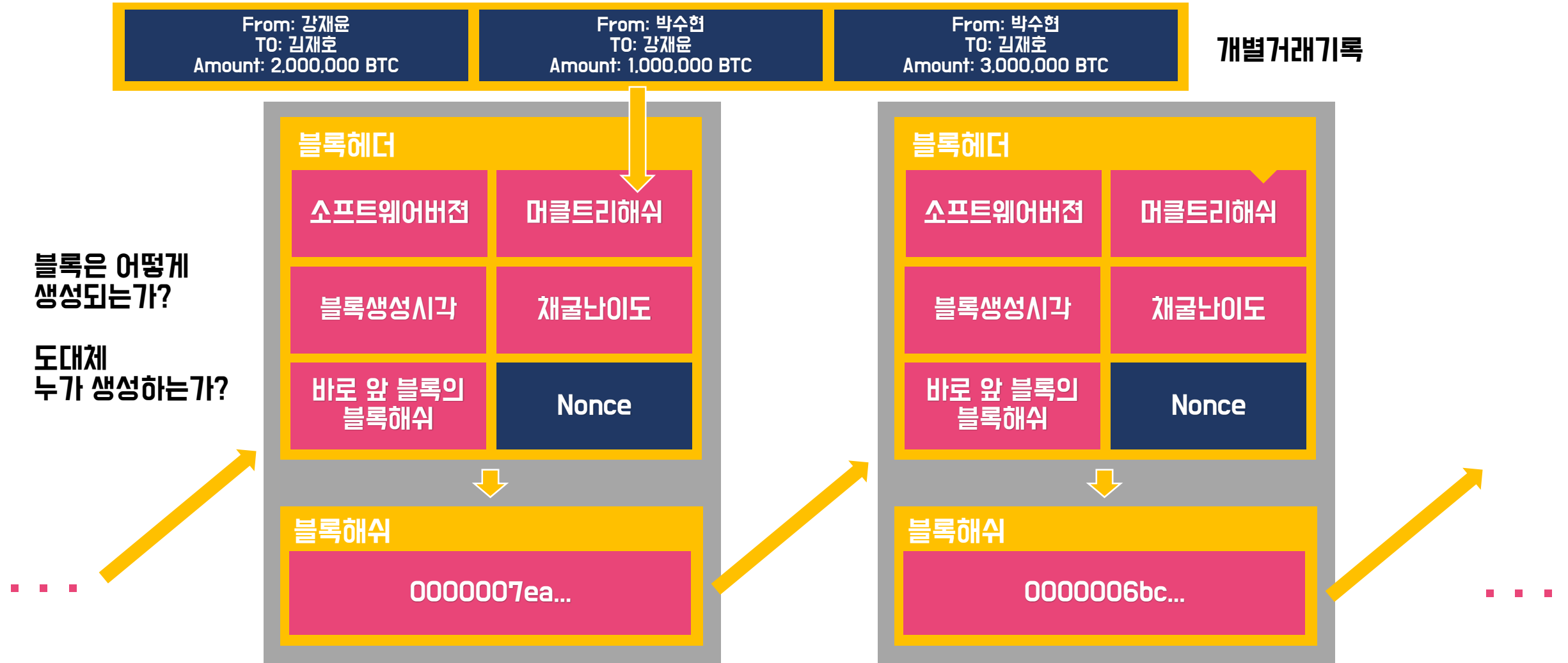
...

...

블록체인 원리



블록체인 원리



블록체인 원리

From: 강재윤
TO: 김재호
Amount: 2,000,000 BTC

From: 박수현
TO: 강재윤
Amount: 1,000,000 BTC

From: 박수현
TO: 김재호
Amount: 3,000,000 BTC

개별거래기록

개별거래기록
으로 부터
머클트리 해쉬를
계산하고.

나머지 5개 값들과
함께 블록해쉬 값을
계산하여 저장하면
블록이 생성된다!

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000007ea...

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

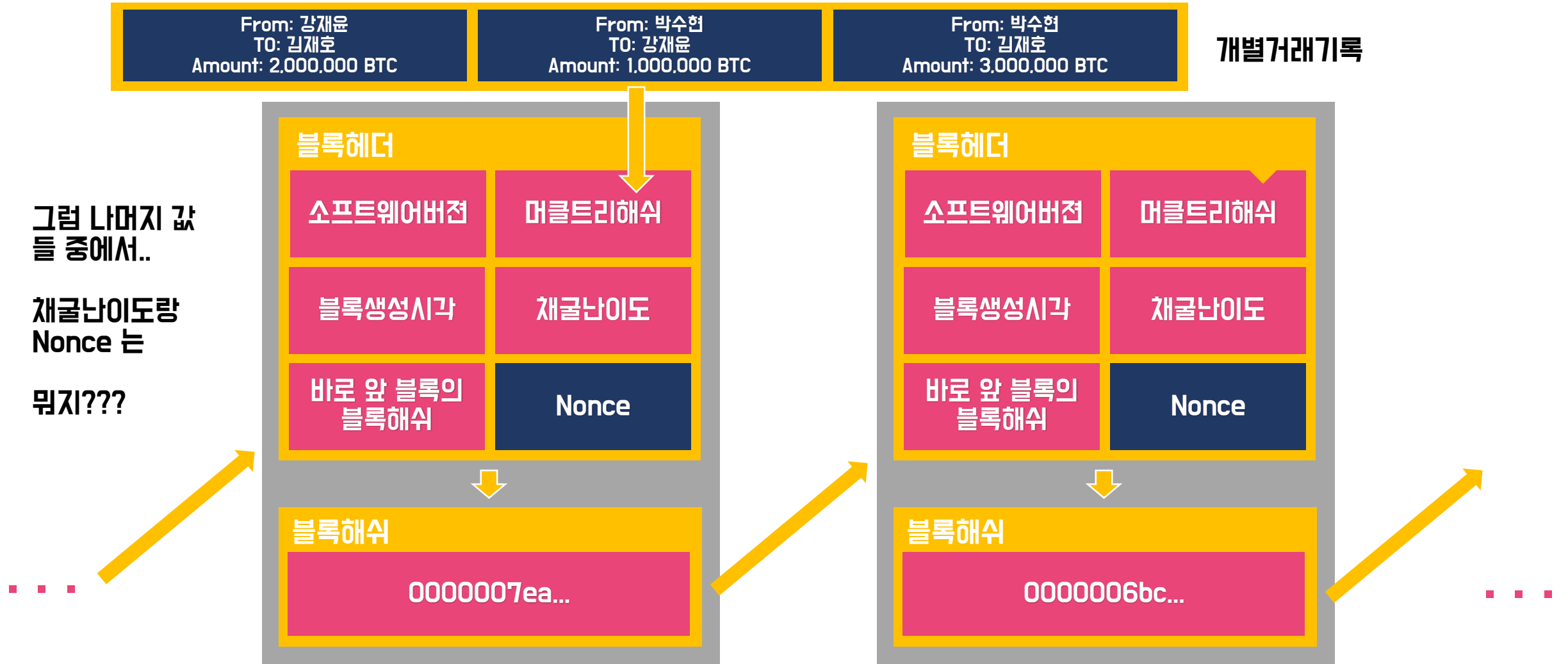
바로 앞 블록의
블록해쉬

Nonce

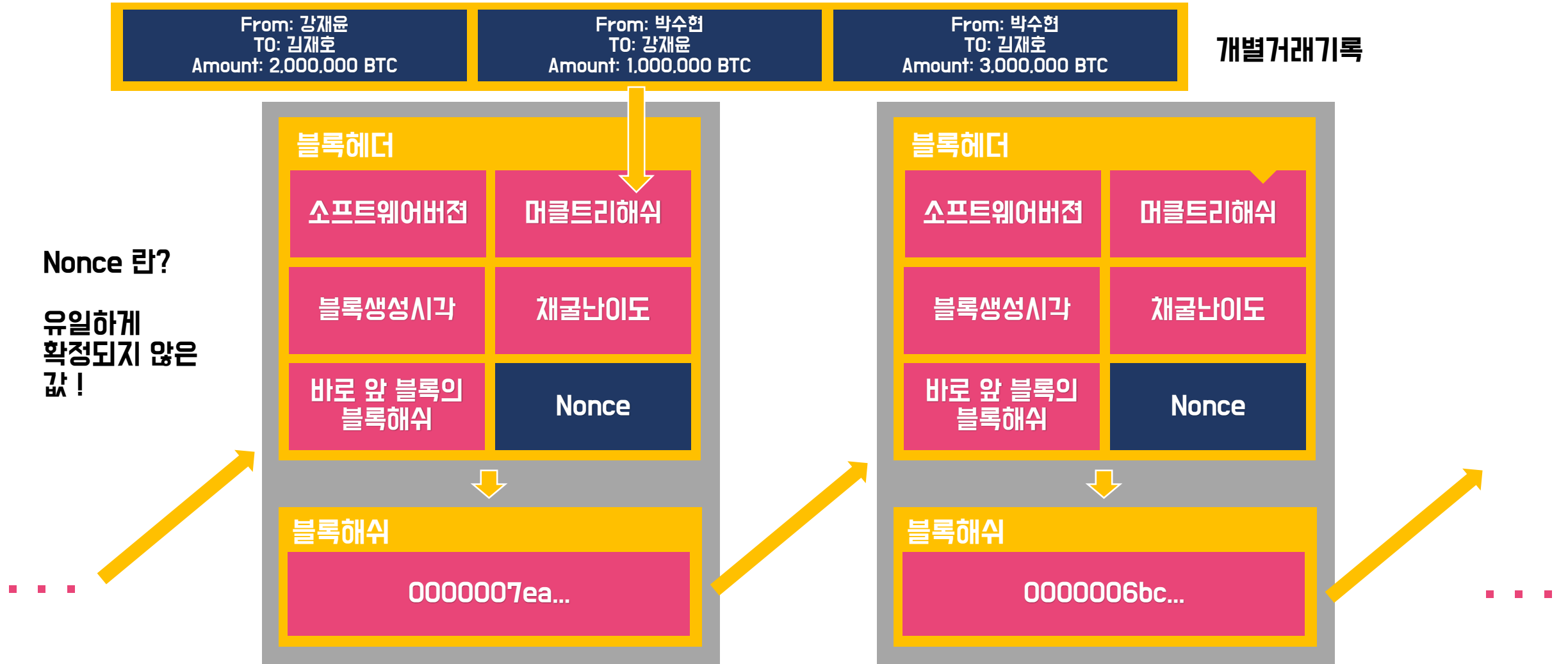
블록해쉬

0000006bc...

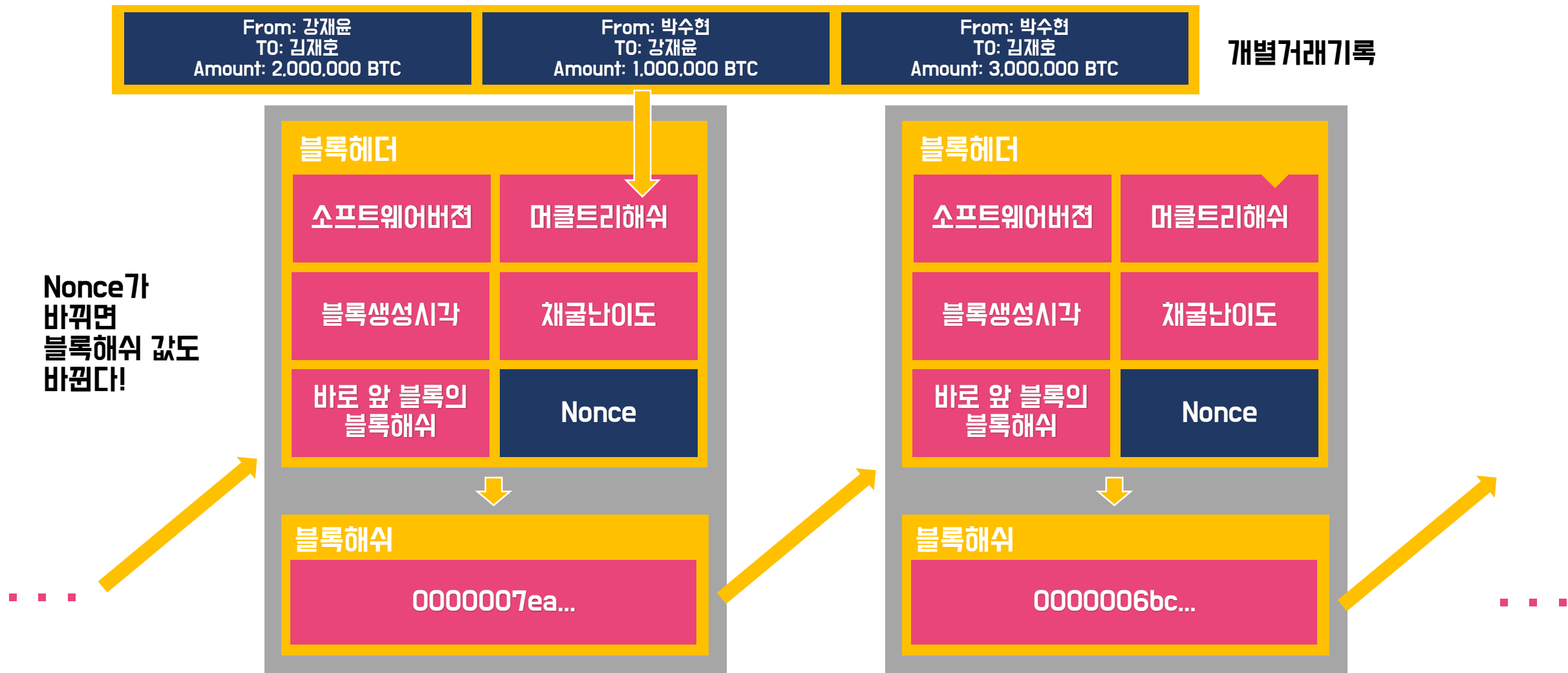
블록체인 원리



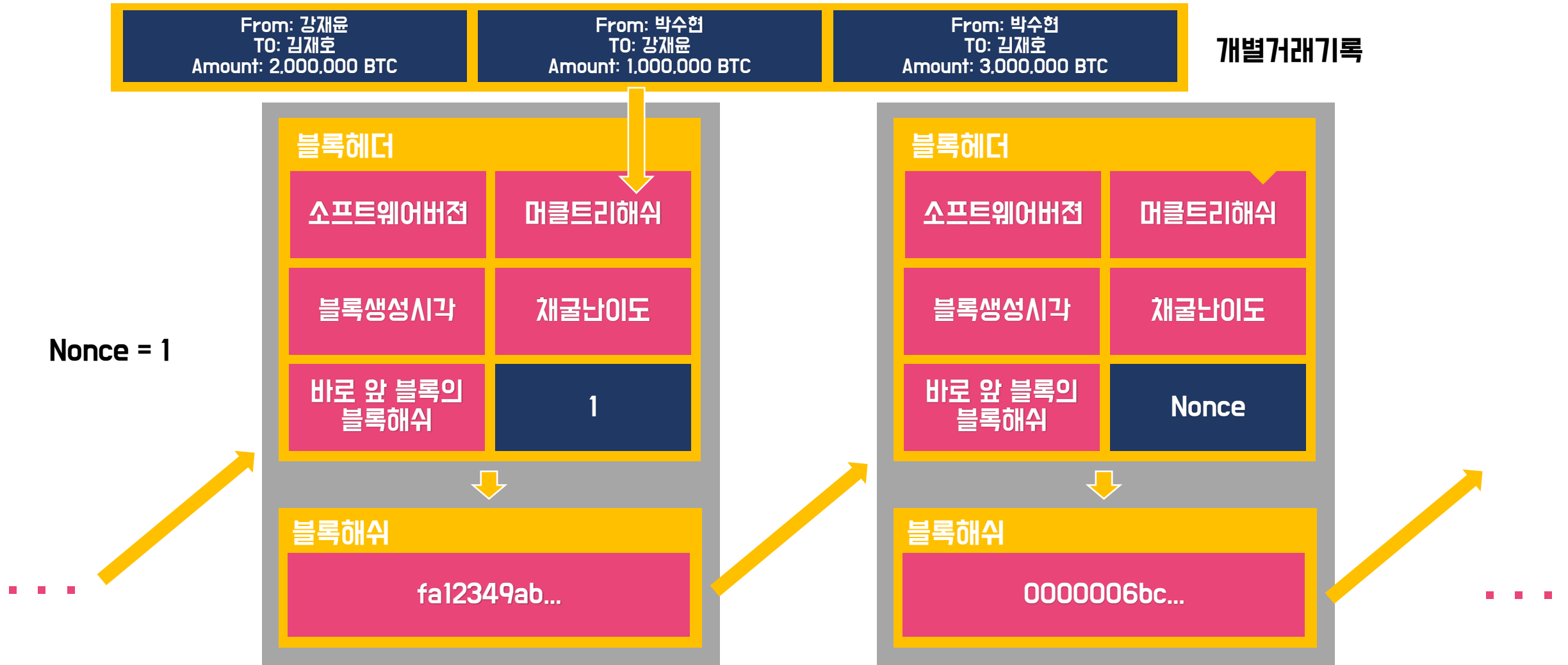
블록체인 원리



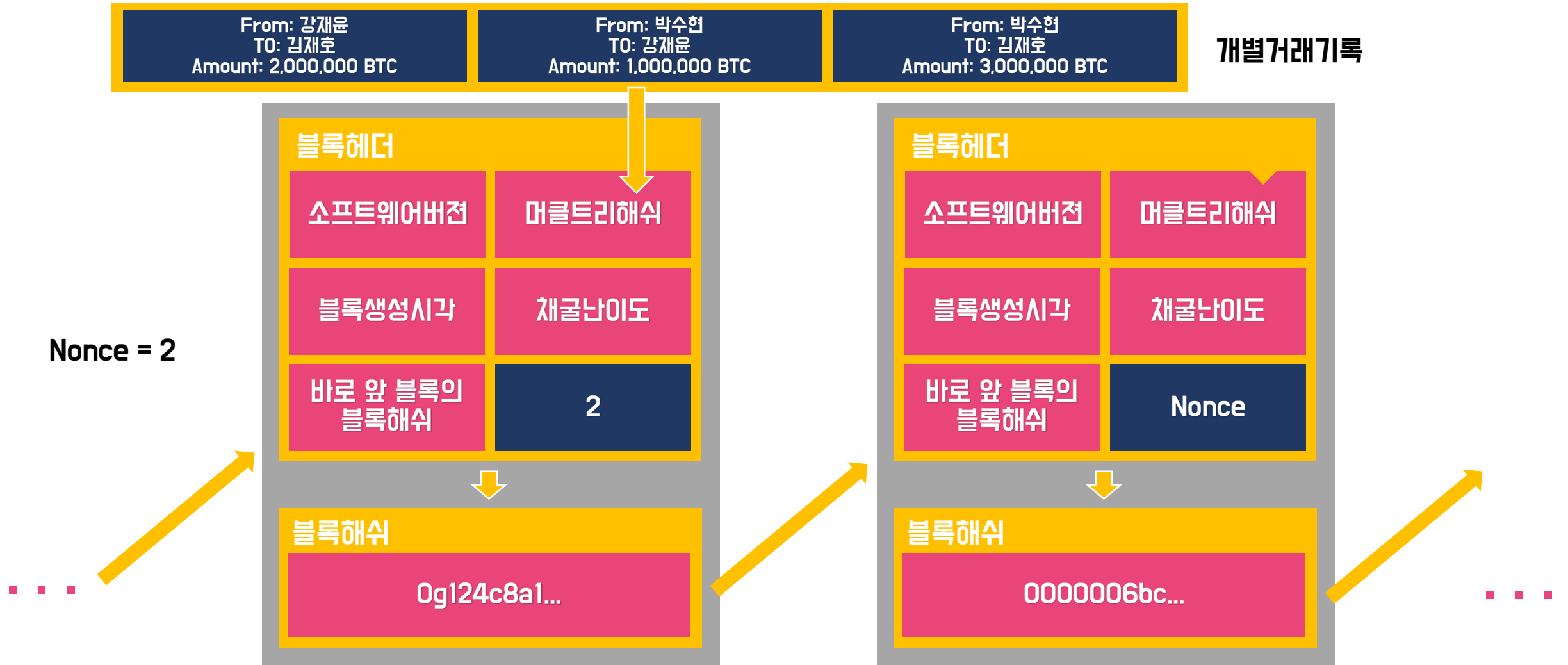
블록체인 원리



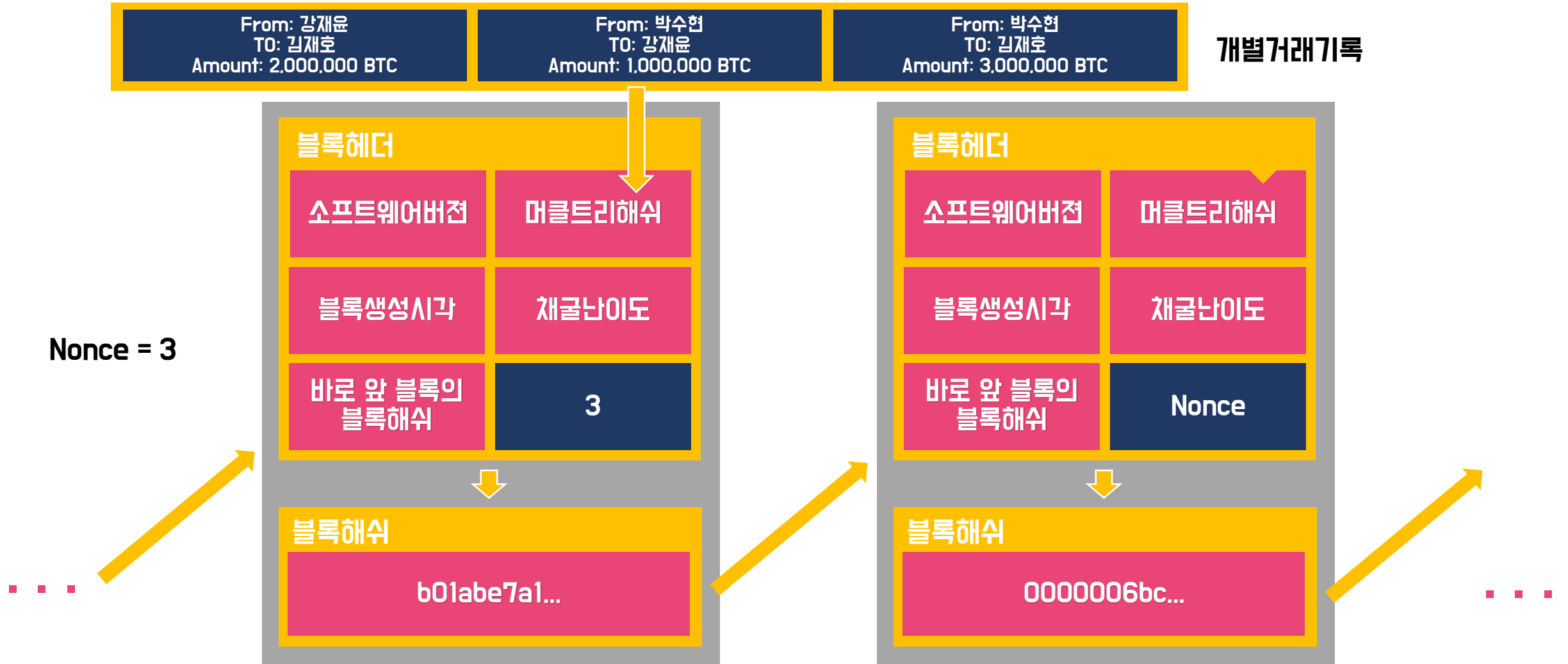
블록체인 원리



블록체인 원리



블록체인 원리



블록체인 원리

From: 강재윤
TO: 김재호
Amount: 2,000,000 BTC

From: 박수현
TO: 강재윤
Amount: 1,000,000 BTC

From: 박수현
TO: 김재호
Amount: 3,000,000 BTC

개별거래기록

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

3

블록해쉬

b01abe7a1...

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000006bc...

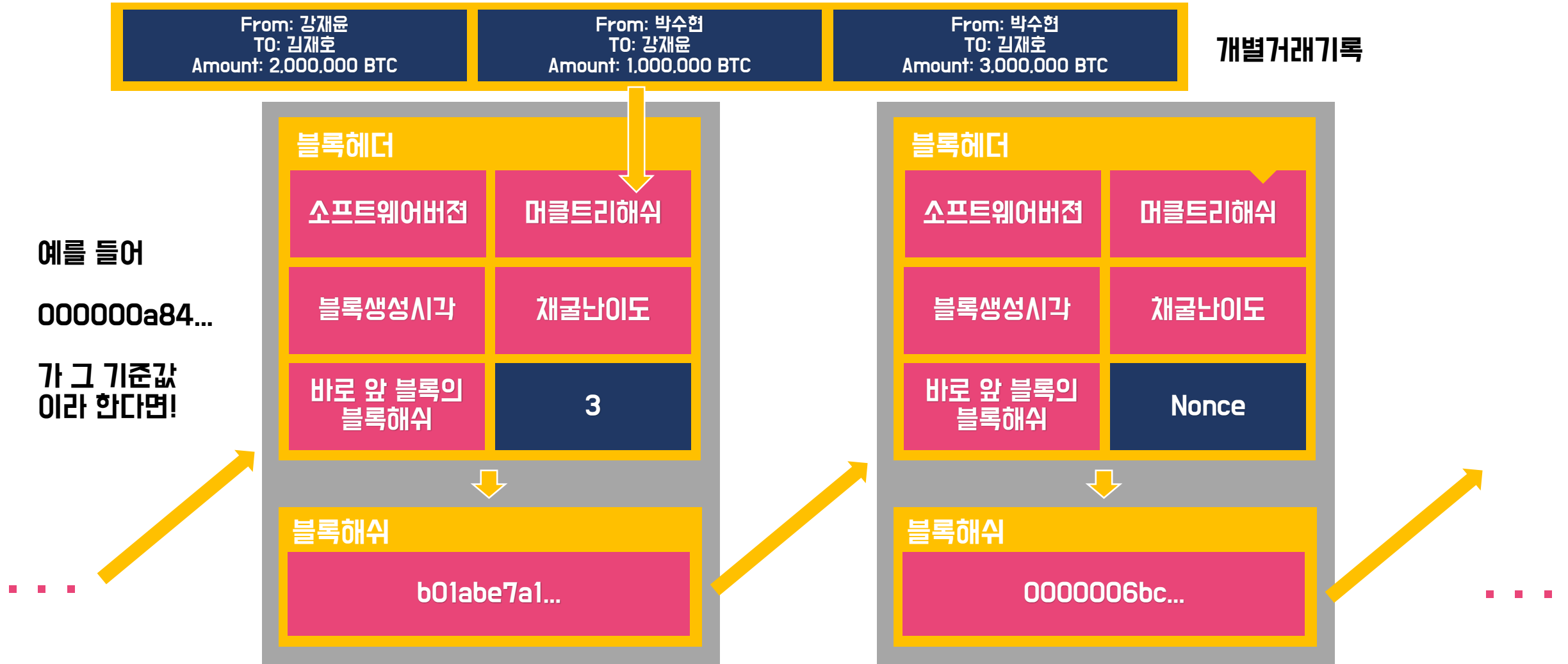
블록해쉬 값은
특정 숫자보다
작아야만 한다!

그래야 블록을
생성할 수 있다!

...

...

블록체인 원리



블록체인 원리

From: 강재윤
TO: 김재호
Amount: 2,000,000 BTC

From: 박수현
TO: 강재윤
Amount: 1,000,000 BTC

From: 박수현
TO: 김재호
Amount: 3,000,000 BTC

개별거래기록

nonce 를
계속하여
바꿔가며

블록해쉬 값이
해당 값보다
작을 때 까지
해쉬값을
계산해야한다!

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

3

블록해쉬

> 000000a84...

b01abe7a1...

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000006bc...

블록체인 원리

From: 강재윤
TO: 김재호
Amount: 2,000,000 BTC

From: 박수현
TO: 강재윤
Amount: 1,000,000 BTC

From: 박수현
TO: 김재호
Amount: 3,000,000 BTC

개별거래기록

nonce 를
계속하여
바꿔가며

블록해쉬 값이
해당 값보다
작을 때 까지
해쉬값을
계산해야한다!

=작업증명

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

3

블록해쉬

> 000000a84...

b01abe7a1...

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000006bc...

블록체인 원리

From: 강재윤
TO: 김재호
Amount: 2,000,000 BTC

From: 박수현
TO: 강재윤
Amount: 1,000,000 BTC

From: 박수현
TO: 김재호
Amount: 3,000,000 BTC

개별거래기록

nonce 를
계속하여
바꿔가며

블록해쉬 값이
해당 값보다
작을 때 까지
해쉬값을
계산해야한다!

=채굴!

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

3

블록해쉬

> 000000a84...

b01abe7a1...

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

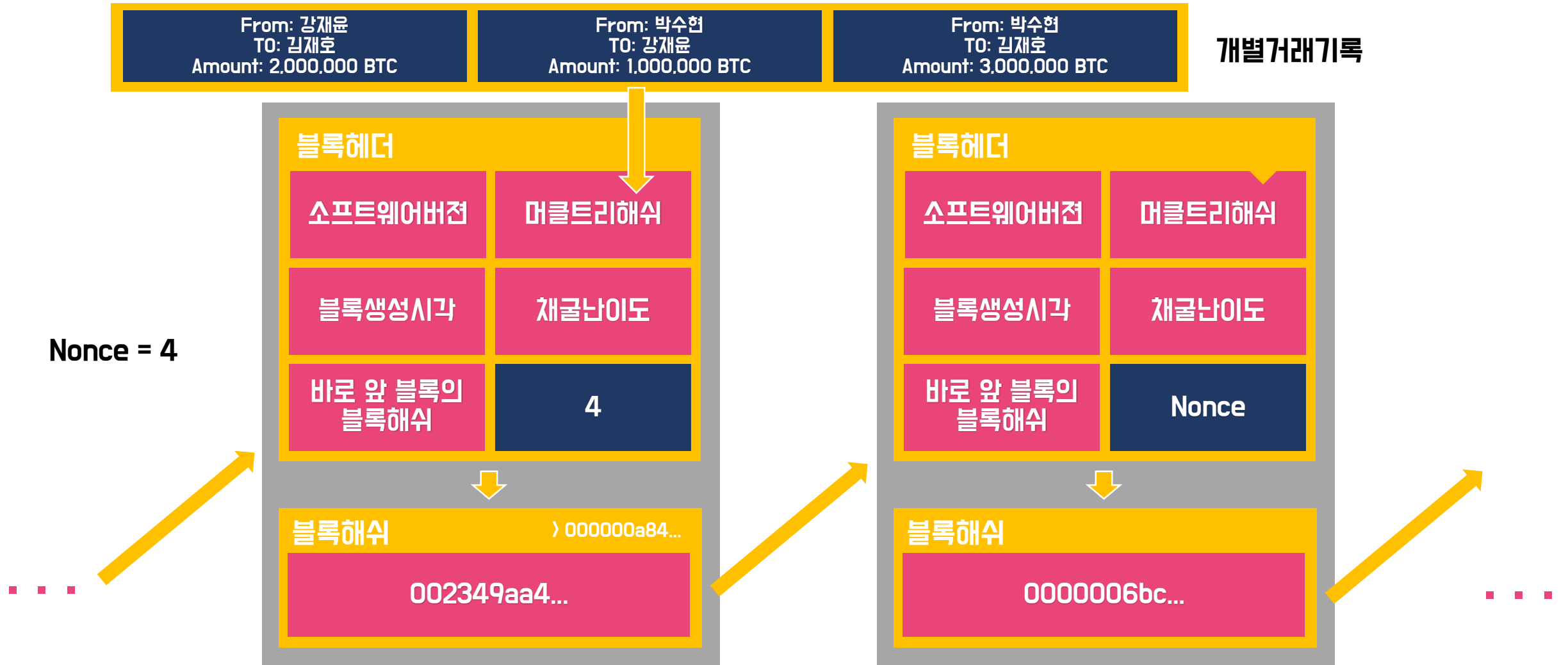
바로 앞 블록의
블록해쉬

Nonce

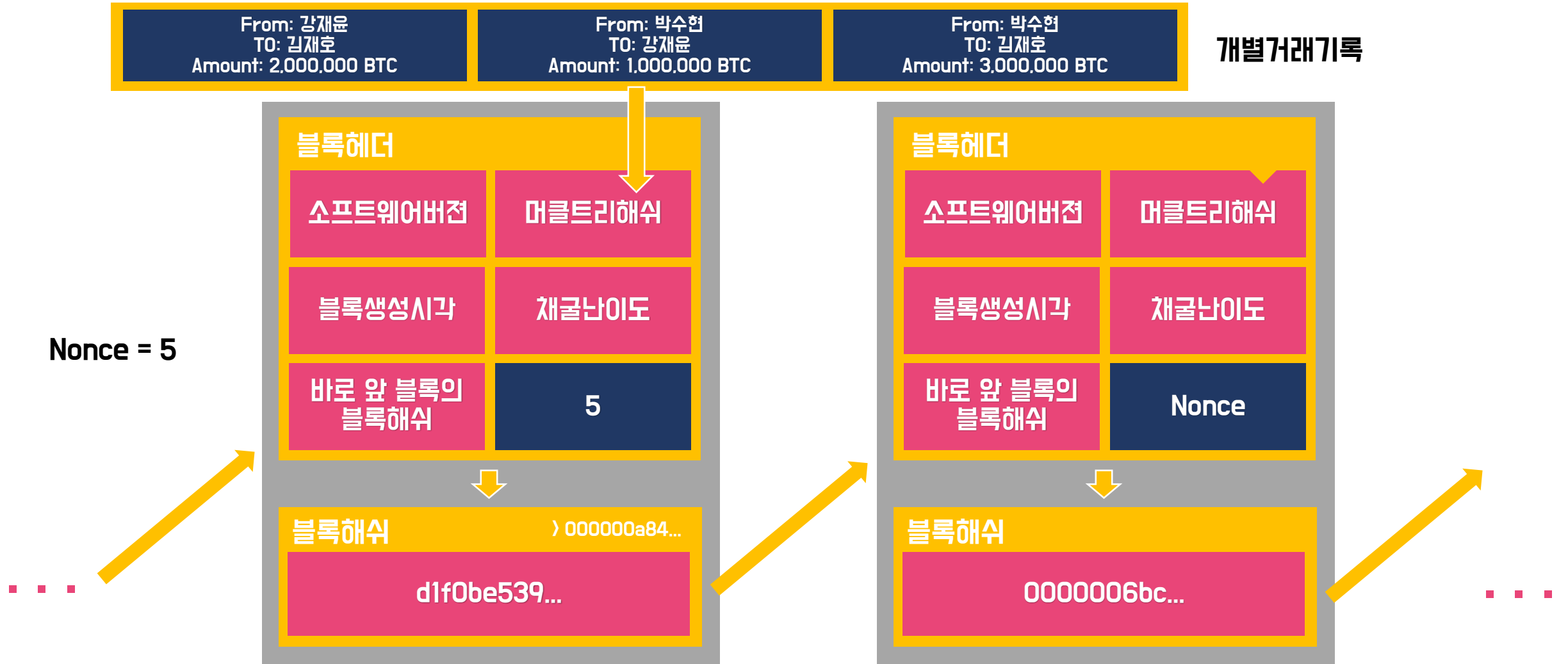
블록해쉬

0000006bc...

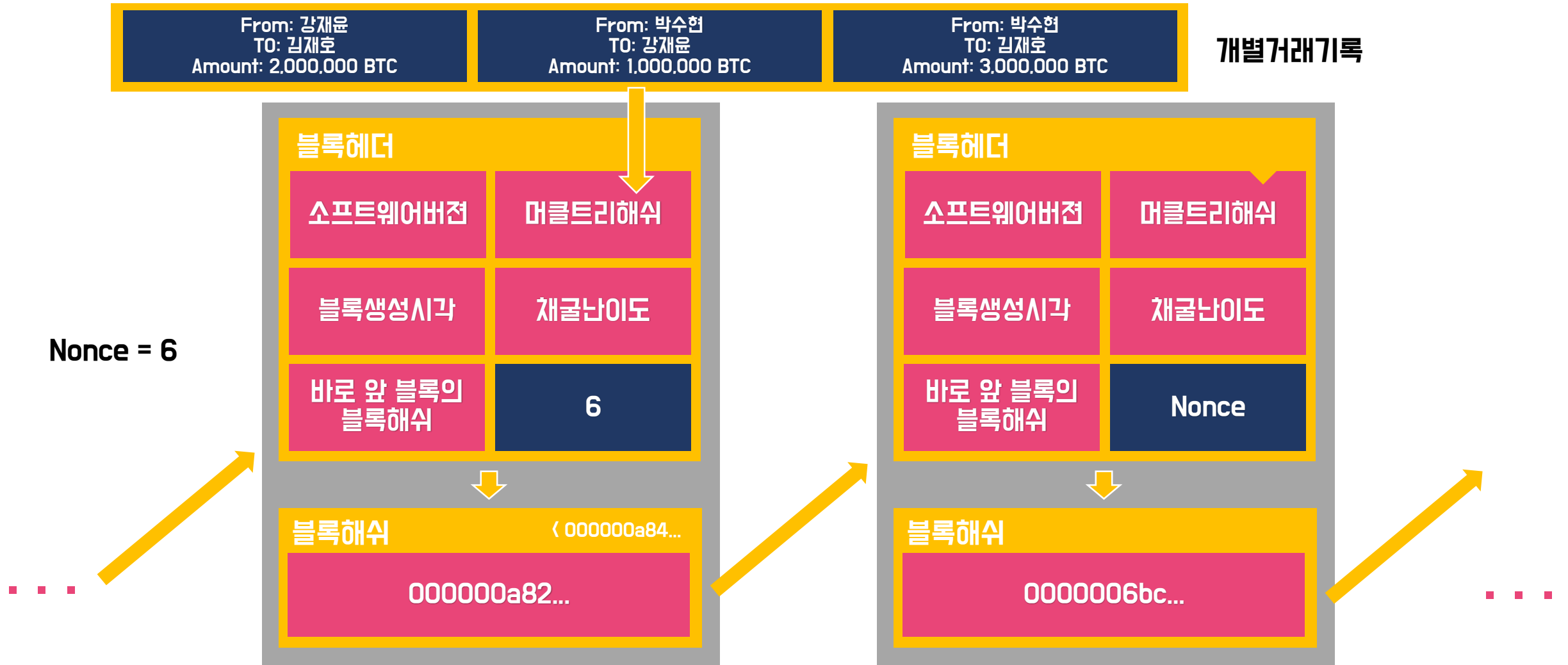
블록체인 원리



블록체인 원리



블록체인 원리



블록체인 원리

From: 강재윤
TO: 김재호
Amount: 2,000,000 BTC

From: 박수현
TO: 강재윤
Amount: 1,000,000 BTC

From: 박수현
TO: 김재호
Amount: 3,000,000 BTC

개별거래기록

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

6

블록해쉬

< 000000a84...

000000a82...

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000006bc...

조건을 만족하는
Nonce 값 (6) 을
찾았다!

블록 생성 성공!

...

...

블록체인 원리

From: 강재윤
TO: 김재호
Amount: 2,000,000 BTC

From: 박수현
TO: 강재윤
Amount: 1,000,000 BTC

From: 박수현
TO: 김재호
Amount: 3,000,000 BTC

개별거래기록

실제로는
엄청나게 많은
Nonce 에 대해
이를 반복해야 함.

블록은 아무나
만드는것이 아니다!

엄청난 컴퓨팅
파워를 사용해야함

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

6

블록해쉬

< 000000a84...

000000a82...

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000006bc...

블록체인 원리

From: 강재운
TO: 김재호
Amount: 2,000,000 BTC

From: 박수현
TO: 강재운
Amount: 1,000,000 BTC

From: 박수현
TO: 김재호
Amount: 3,000,000 BTC

개별거래기록

실제로는
엄청나게 많은
Nonce 에 대해
이를 반복해야 함.

블록은 아무나
만드는것이 아니다!

엄청난 컴퓨팅
파워를 사용해야함

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

6

블록해쉬

< 000000a84...

000000a82...



GPU 대란!

블록체인 원리

From: 강재윤
TO: 김재호
Amount: 2,000,000 BTC

From: 박수현
TO: 강재윤
Amount: 1,000,000 BTC

From: 박수현
TO: 김재호
Amount: 3,000,000 BTC

개별거래기록

실제로는
엄청나게 많은
Nonce 에 대해
이를 반복해야 함.

블록은 아무나
만드는것이 아니다!

엄청난 컴퓨팅
파워를 사용해야함

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

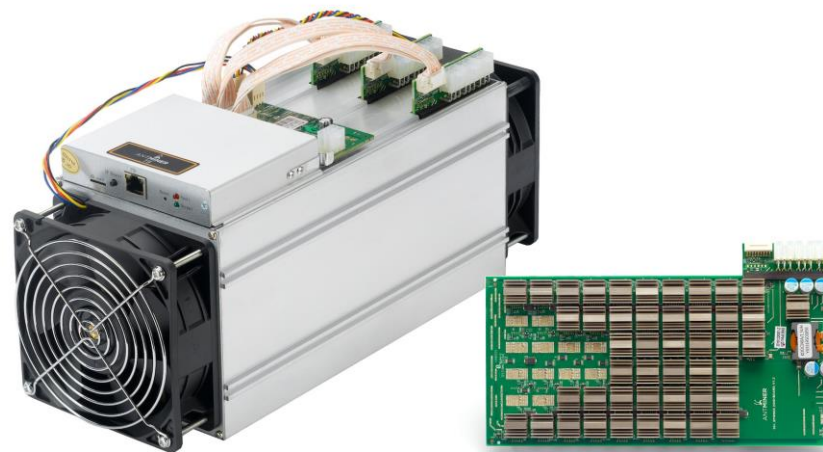
바로 앞 블록의
블록해쉬

6

블록해쉬

< 000000a84...

000000a82...



ASIC 채굴기의 등장

블록체인 원리

From: 강재운
TO: 김재호
Amount: 2,000,000 BTC

From: 박수현
TO: 강재운
Amount: 1,000,000 BTC

From: 박수현
TO: 김재호
Amount: 3,000,000 BTC

개별거래기록

실제로는
엄청나게 많은
Nonce 에 대해
이를 반복해야 함.

블록은 아무나
만드는것이 아니다!

엄청난 컴퓨팅
파워를 사용해야함

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

6

블록해쉬

< 000000a84...

000000a82...



비트코인 채굴장
in 중국

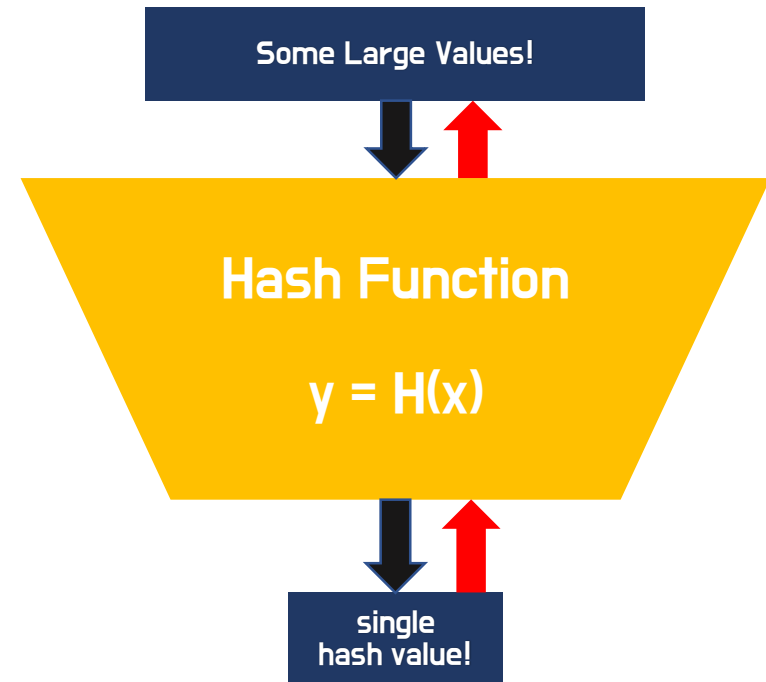
블록체인 원리

From: 강재윤 TO: 김재호 Amount: 2,000,000 BTC	From: 박수현 TO: 강재윤 Amount: 1,000,000 BTC	From: 박수현 TO: 김재호 Amount: 3,000,000 BTC
---	---	---

개별거래기록

충분히 작은
해쉬 값
ex) 000000a81..
을 먼저 만들고

역함수를 이용하여
Nonce를 찾는건?



블록체인 원리

From: 강재윤 TO: 김재호 Amount: 2,000,000 BTC	From: 박수현 TO: 강재윤 Amount: 1,000,000 BTC	From: 박수현 TO: 김재호 Amount: 3,000,000 BTC
---	---	---

개별거래기록

불가능!!

Secure
Hash
Algorithm

'SHA' 를 사용하여
단방향 계산만 가능

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

6

블록해쉬

< 000000a84...

000000a82...

Some Large Values!

SHA-256

single
hash value!

블록체인 원리

From: 강재윤
TO: 김재호
Amount: 2,000,000 BTC

From: 박수현
TO: 강재윤
Amount: 1,000,000 BTC

From: 박수현
TO: 김재호
Amount: 3,000,000 BTC

개별거래기록

그럼 이렇게
시간도 써야하고
컴퓨팅자원도
써야하는..

'채굴'
이라는 작업을

누가? 왜?
하는가?

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

6

블록해쉬

< 000000a84...

000000a82...

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

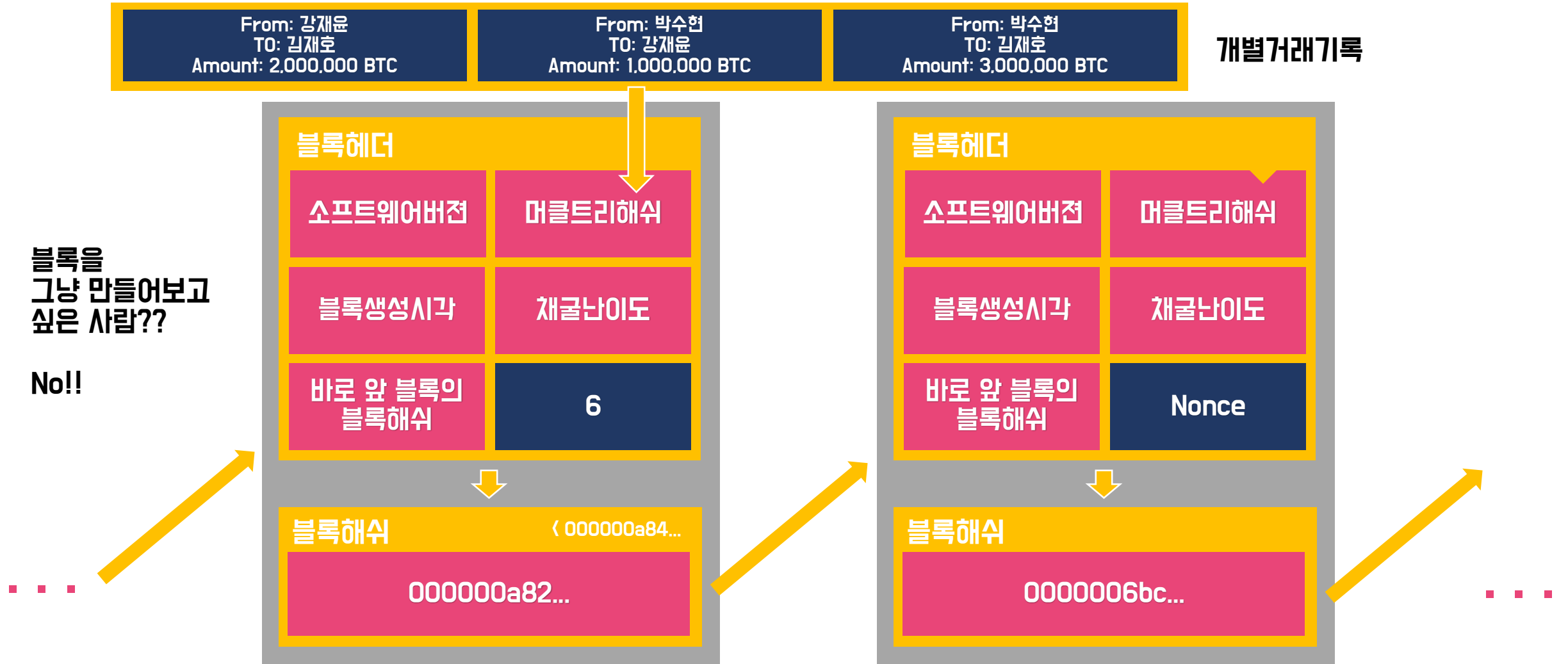
바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000006bc...

블록체인 원리



블록체인 원리

From: 강재윤
TO: 김재호
Amount: 2,000,000 BTC

From: 박수현
TO: 강재윤
Amount: 1,000,000 BTC

From: 박수현
TO: 김재호
Amount: 3,000,000 BTC

개별거래기록

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

6

블록해쉬

< 000000a84...

000000a82...

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000006bc...

단순히 자발적
동기에만 의지하면
블록체인 및
비트코인 시스템은
유지가 불가능하다.

블록을 만드는
사람이 없을테니!

...

...

블록체인 원리

From: 강재윤
TO: 김재호
Amount: 2,000,000 BTC

From: 박수현
TO: 강재윤
Amount: 1,000,000 BTC

From: 박수현
TO: 김재호
Amount: 3,000,000 BTC

개별거래기록

그 동기는!

블록을 만들면
BTC를 발행해서
생성자에게 제공!

블록 안에 담긴
거래기록들의
수수료도 제공!

블록헤더

소프트

해쉬

바이트

블록해쉬

0000000a82...

0000a84...

블록헤더

소프트

해쉬

바이트

블록해쉬

00000000...

...

...

블록체인 원리

From: 강재윤
TO: 김재호
Amount: 2,000,000 BTC

From: 박수현
TO: 강재윤
Amount: 1,000,000 BTC

From: 박수현
TO: 김재호
Amount: 3,000,000 BTC

개별거래기록

그렇다면..
채굴자들이
많아지고.

컴퓨팅 성능이
좋아져서

BTC가 수 없이
발행되면??

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

6

블록해쉬

< 000000a84...

000000a82...

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000006bc...

블록체인 원리

From: 강재윤
TO: 김재호
Amount: 2,000,000 BTC

From: 박수현
TO: 강재윤
Amount: 1,000,000 BTC

From: 박수현
TO: 김재호
Amount: 3,000,000 BTC

개별거래기록

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

6

블록해쉬

< 000000a84...

000000a82...

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000006bc...

난이도 조절을
통해 이러한
현상을 막는다!

채굴난이도 = ?

...

...

블록체인 원리

From: 강재윤
TO: 김재호
Amount: 2,000,000 BTC

From: 박수현
TO: 강재윤
Amount: 1,000,000 BTC

From: 박수현
TO: 김재호
Amount: 3,000,000 BTC

개별거래기록

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

6

블록해쉬

< 000000a84...

000000a82...

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000006bc...

블록해쉬가
특정 값보다
작아야 한다면..

이 특정 값이
작으면 작을수록
채굴이 어렵다!

...

...

블록체인 원리

From: 강재윤
TO: 김재호
Amount: 2,000,000 BTC

From: 박수현
TO: 강재윤
Amount: 1,000,000 BTC

From: 박수현
TO: 김재호
Amount: 3,000,000 BTC

개별거래기록

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

6

블록해쉬

< 000000064...

000000a82...

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000006bc...

즉, 블록이
많이 생성되면
이 기준 숫자를
낮게 낮추어서
채굴난이도를 높인다!

...

...

블록체인 원리

From: 강재윤
TO: 김재호
Amount: 2,000,000 BTC

From: 박수현
TO: 강재윤
Amount: 1,000,000 BTC

From: 박수현
TO: 김재호
Amount: 3,000,000 BTC

개별거래기록

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000007ea...

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000006bc...

2160개의 블록
생성을 단위로
채굴난이도를 조절!

...

...

블록체인 원리

From: 강재윤
TO: 김재호
Amount: 2,000,000 BTC

From: 박수현
TO: 강재윤
Amount: 1,000,000 BTC

From: 박수현
TO: 김재호
Amount: 3,000,000 BTC

개별거래기록

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000007ea...

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000006bc...

21600 분 동안
2160개의 블록생성
을 기준으로
채굴난이도를 조절!

= 1블록/10분

...

...

블록체인 원리

From: 강재윤
TO: 김재호
Amount: 2,000,000 BTC

From: 박수현
TO: 강재윤
Amount: 1,000,000 BTC

From: 박수현
TO: 김재호
Amount: 3,000,000 BTC

개별거래기록

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000007ea...

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000006bc...

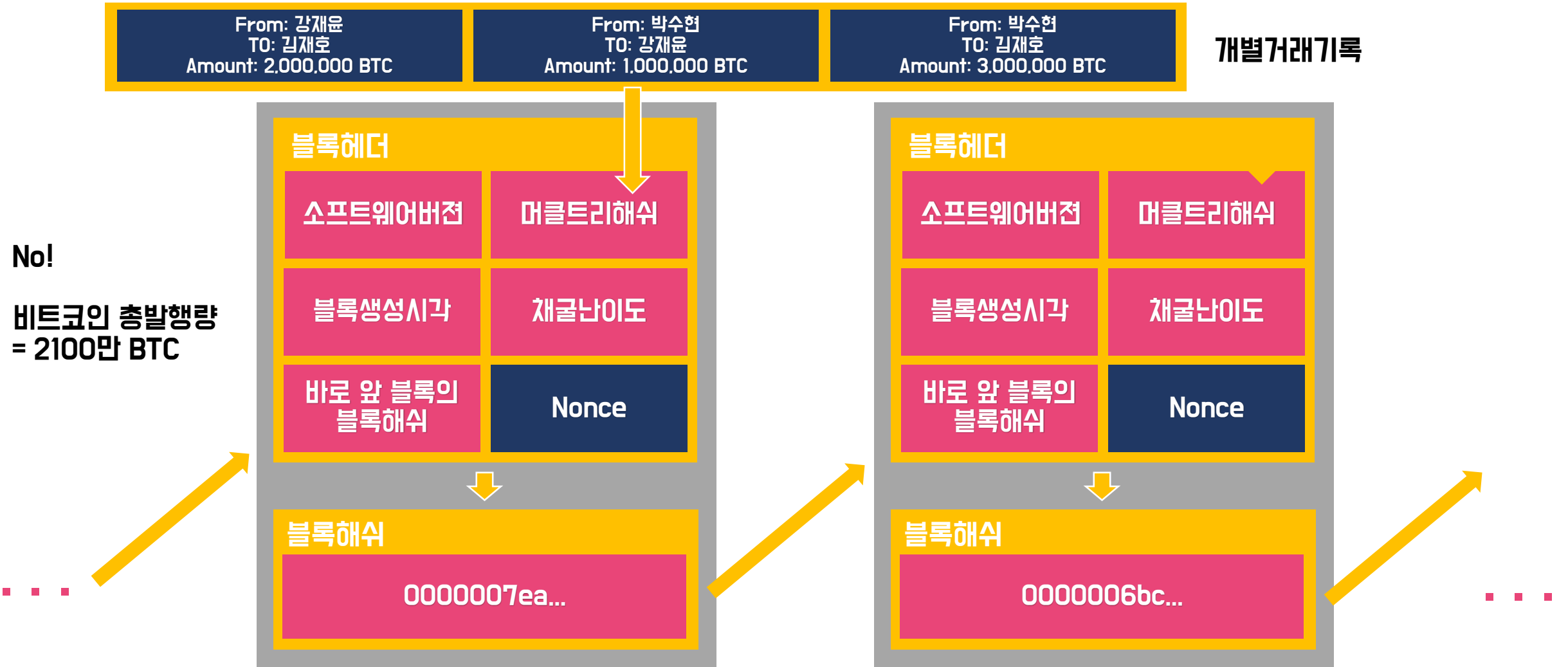
그럼 이렇게
계속해서 BTC
를 발행하다 보면,

총 발행량이 무한대?

...

...

블록체인 원리



블록체인 원리

From: 강재윤
TO: 김재호
Amount: 2,000,000 BTC

From: 박수현
TO: 강재윤
Amount: 1,000,000 BTC

From: 박수현
TO: 김재호
Amount: 3,000,000 BTC

개별거래기록

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000007ea...

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000006bc...

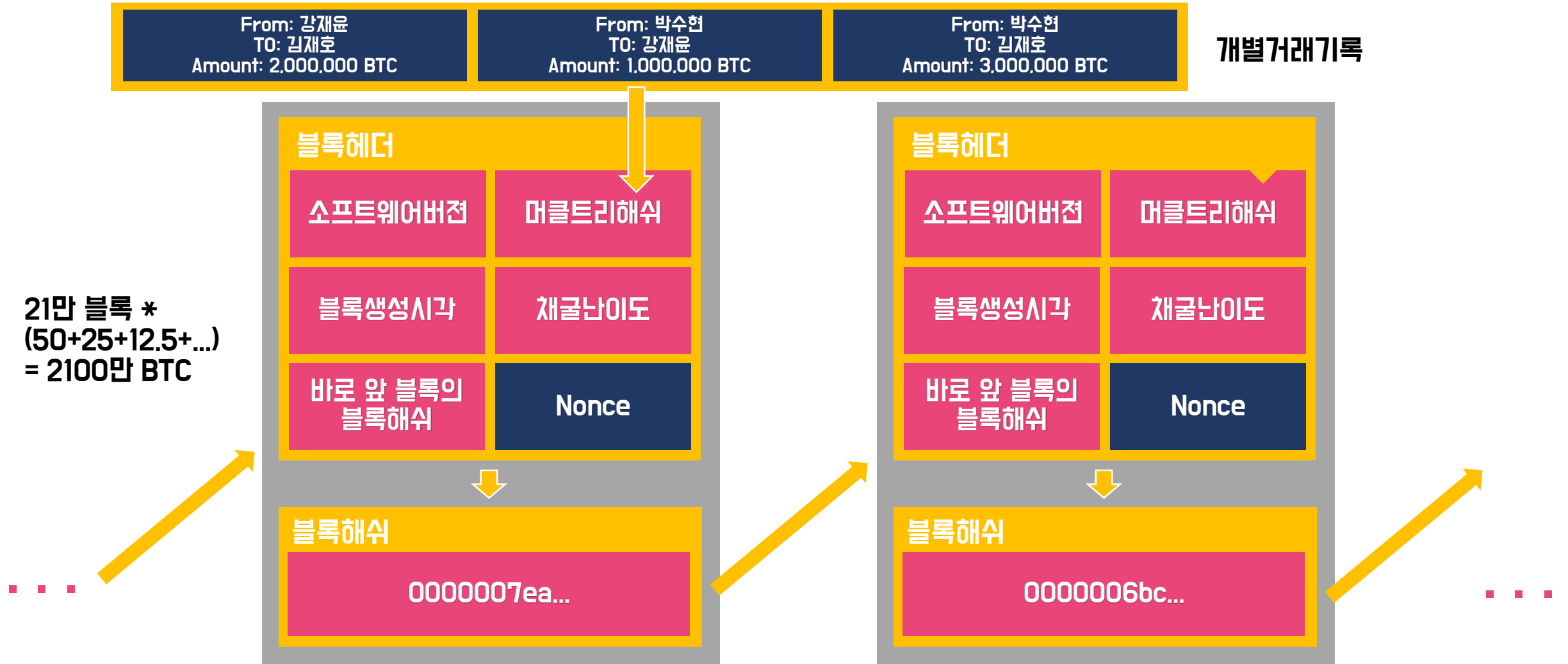
이를 위해
초기 블록에 대해
50BTC 발행을
시작으로.

21만 블록 생성 마다
보상 BTC 발행을
절반으로 줄인다!

...

...

블록체인 원리



블록체인 원리

From: 강재윤
TO: 김재호
Amount: 2,000,000 BTC

From: 박수현
TO: 강재윤
Amount: 1,000,000 BTC

From: 박수현
TO: 김재호
Amount: 3,000,000 BTC

개별거래기록

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000007ea...

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000006bc...

그럼 나중에는..
보상으로
수수료만 받는
날이 온다!

...

...

블록체인 원리

From: 강재윤
TO: 김재호
Amount: 2,000,000 BTC

From: 박수현
TO: 강재윤
Amount: 1,000,000 BTC

From: 박수현
TO: 김재호
Amount: 3,000,000 BTC

개별거래기록

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000007ea...

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000006bc...

그러나..
채굴업자 입장에선
총 비용보다
수익이 커야만
하기 때문에..

...

...

블록체인 원리

From: 강재윤
TO: 김재호
Amount: 2,000,000 BTC

From: 박수현
TO: 강재윤
Amount: 1,000,000 BTC

From: 박수현
TO: 김재호
Amount: 3,000,000 BTC

개별거래기록

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000007ea...

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000006bc...

수수료를
증가시킨다 ?

대폭 높아지기는
어렵다!

...

...

블록체인 원리

From: 강재윤
TO: 김재호
Amount: 2,000,000 BTC

From: 박수현
TO: 강재윤
Amount: 1,000,000 BTC

From: 박수현
TO: 김재호
Amount: 3,000,000 BTC

개별거래기록

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000007ea...

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000006bc...

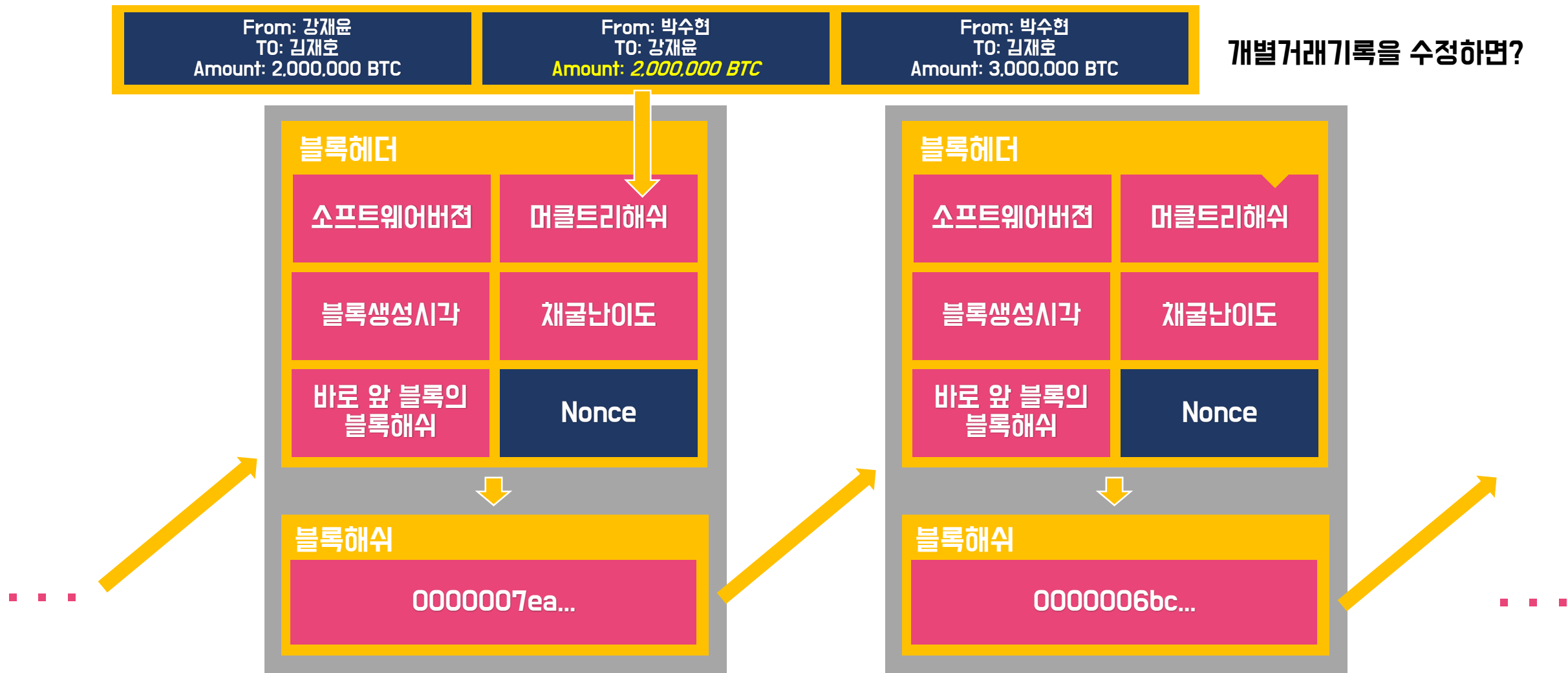
채굴비용감소!

BTC 발행이
끝나는 2140년 경에는
채굴난이도가
낮아질 예정

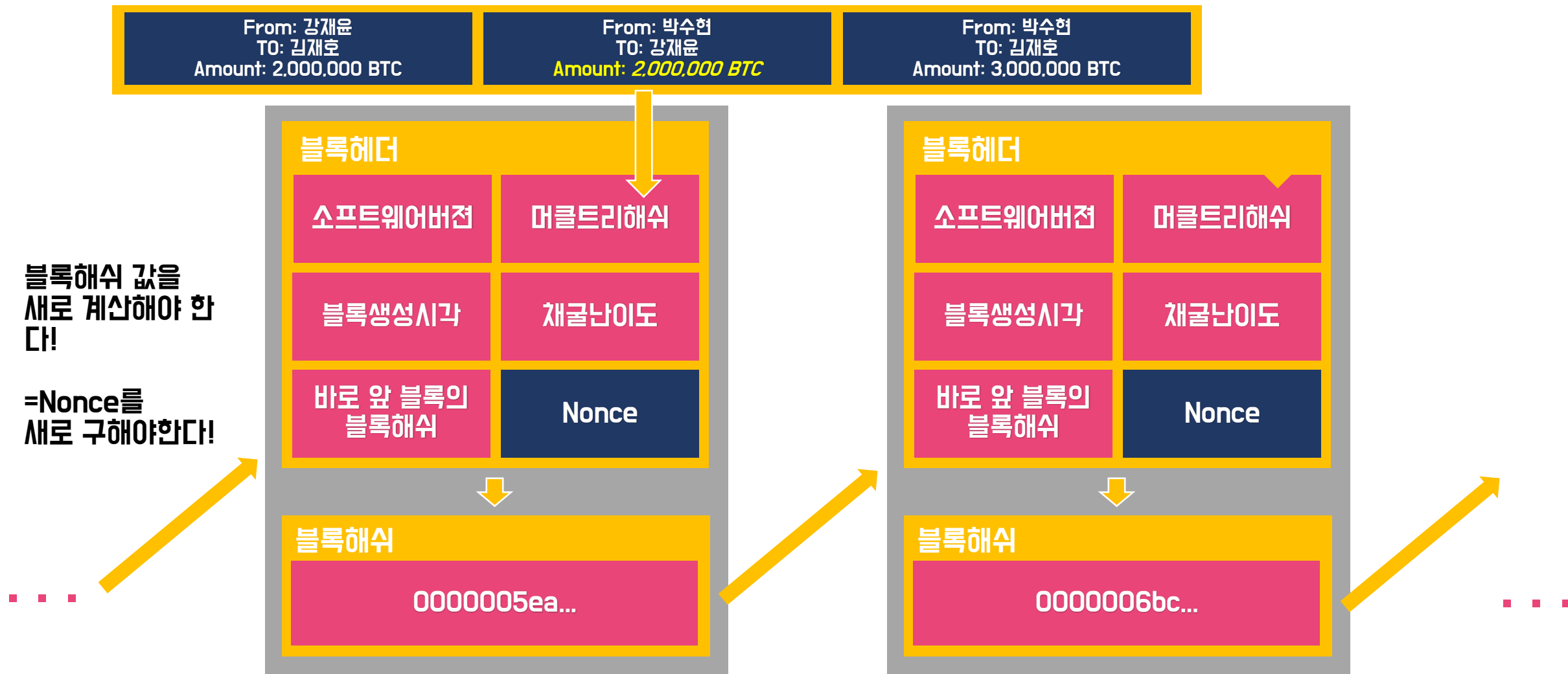
...

...

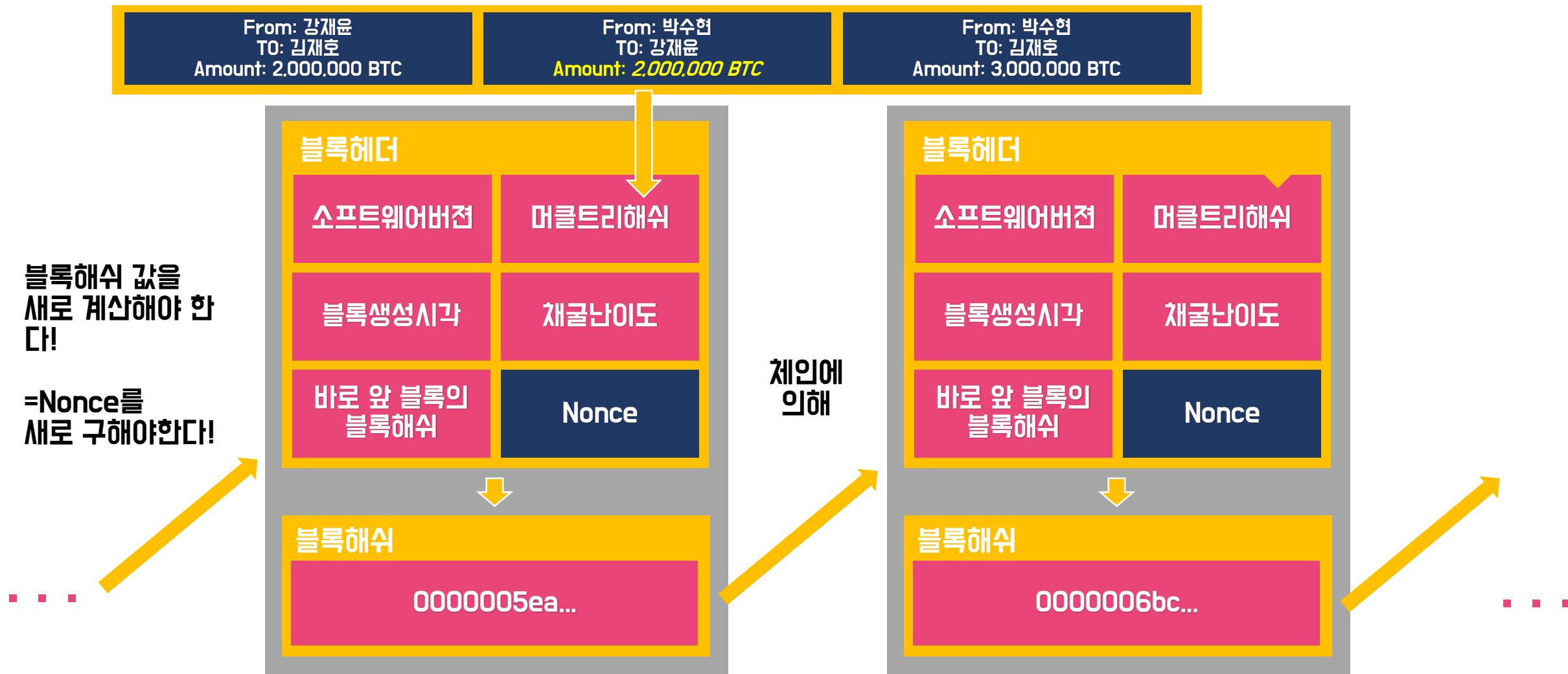
블록체인 원리



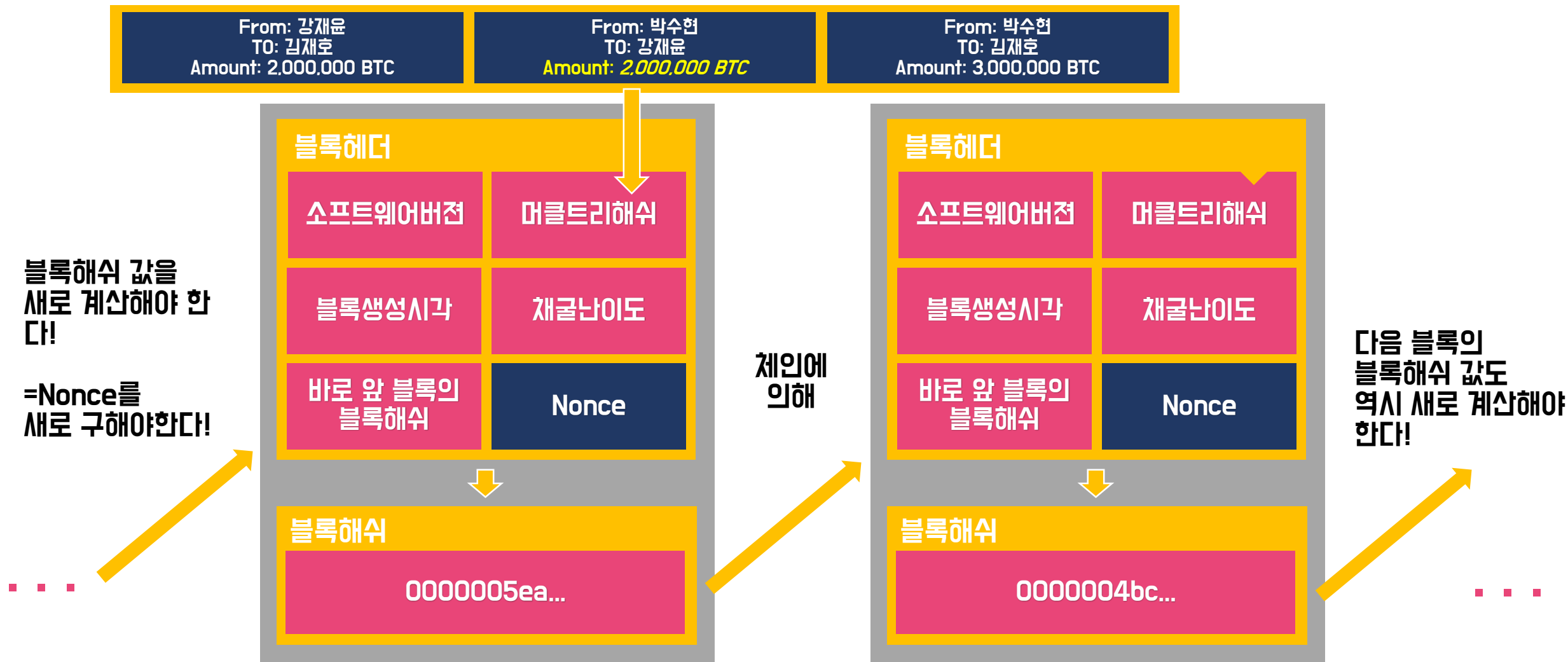
블록체인 원리



블록체인 원리



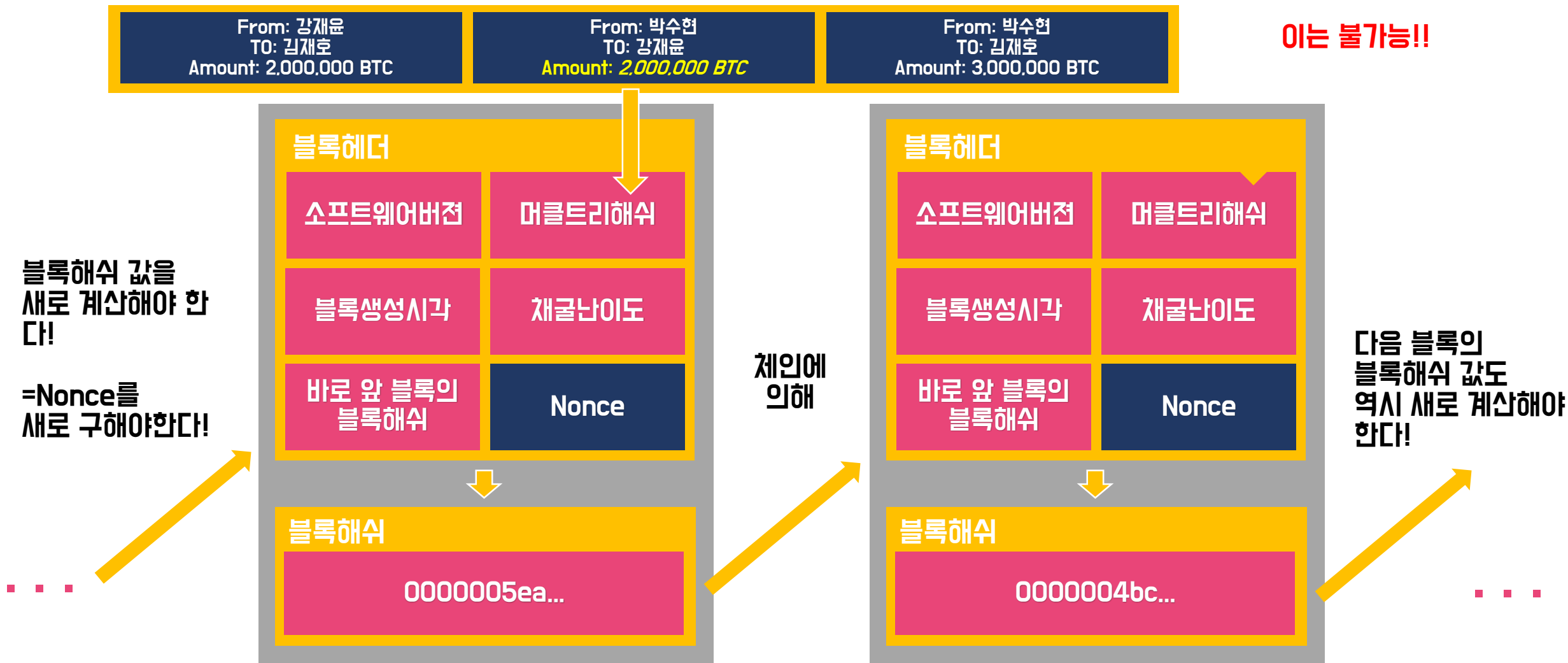
블록체인 원리



블록체인 원리

사실 상 뒤에 있는
모든 블록해쉬 값을
다시 구해야 하는데

이는 불가능!!



블록체인 원리

중요!
완료된 거래는
조작이 불가능!!

From: 강재운
TO: 김재호
Amount: 2,000,000 BTC

From: 박수현
TO: 강재운
Amount: 2,000,000 BTC

From: 박수현
TO: 김재호
Amount: 3,000,000 BTC

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000005ea...

블록헤더

소프트웨어버전

머클트리해쉬

블록생성시각

채굴난이도

바로 앞 블록의
블록해쉬

Nonce

블록해쉬

0000004bc...

체인에
의해

블록해쉬 값을
새로 계산해야 한
다!

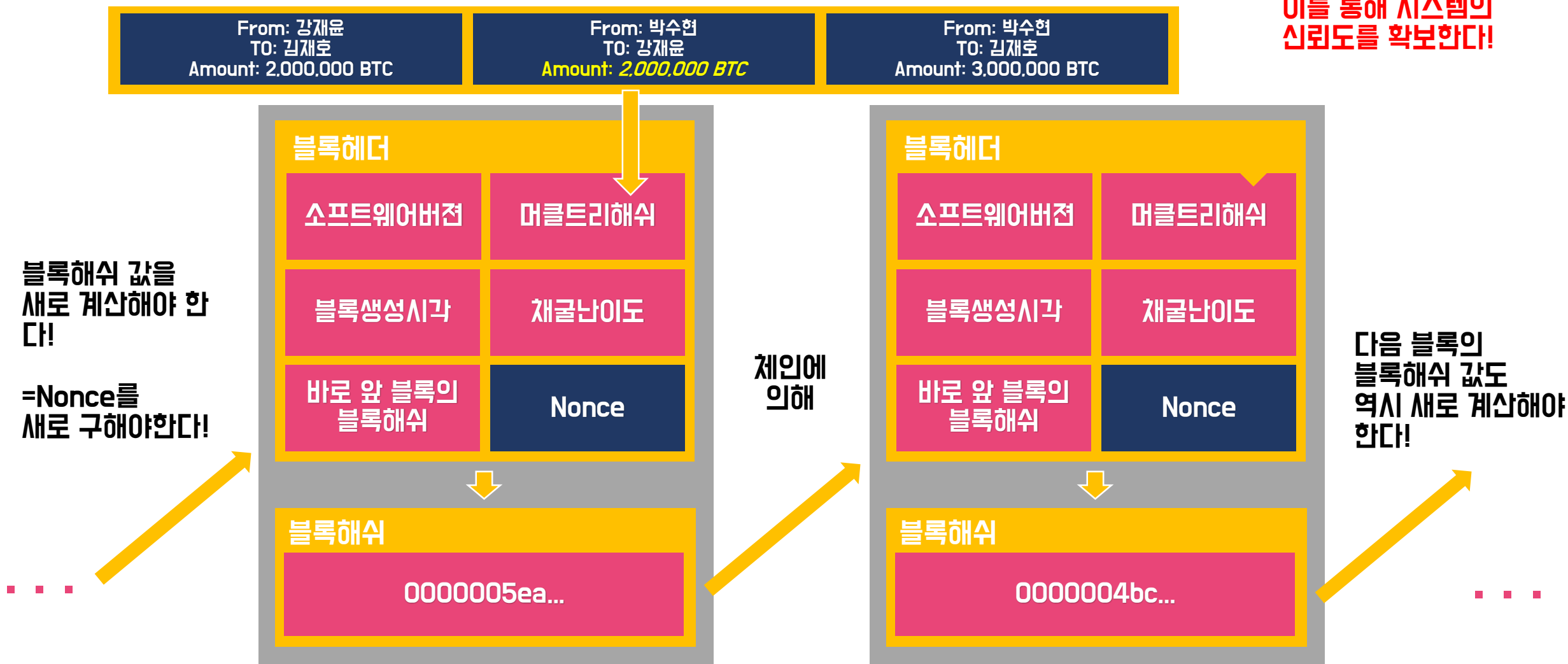
=Nonce를
새로 구해야한다!

다음 블록의
블록해쉬 값도
역시 새로 계산해야
한다!

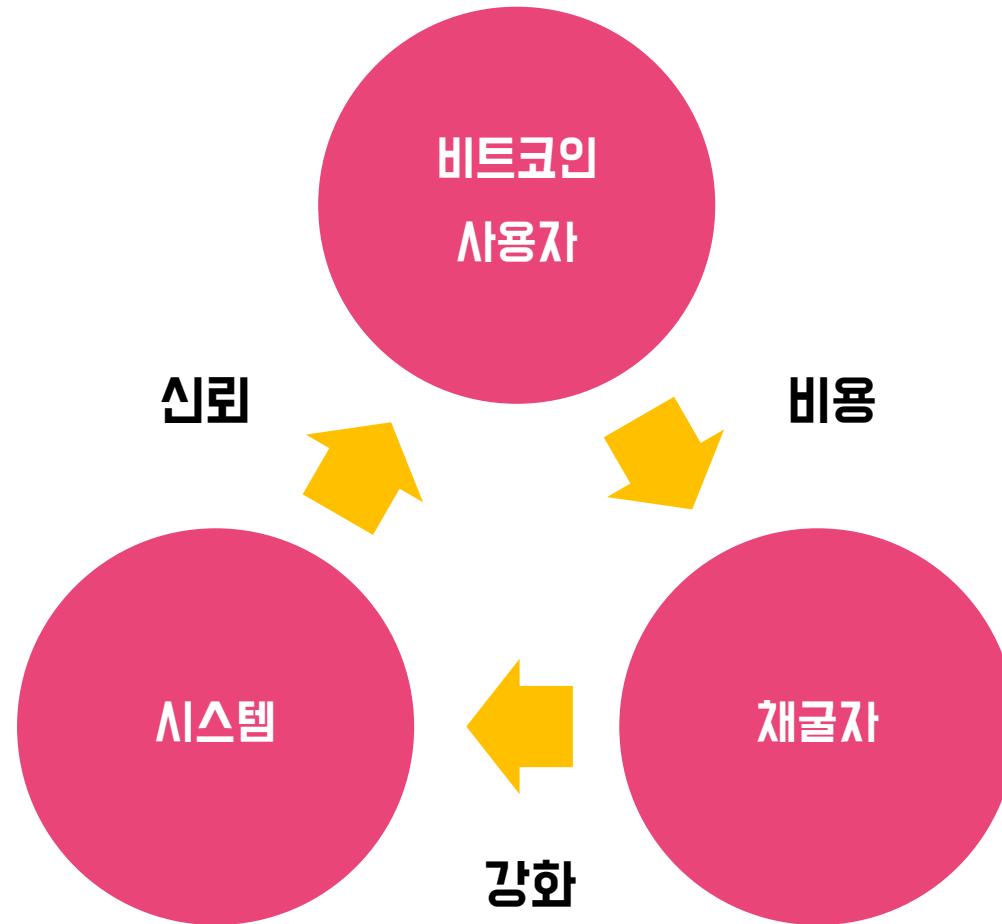
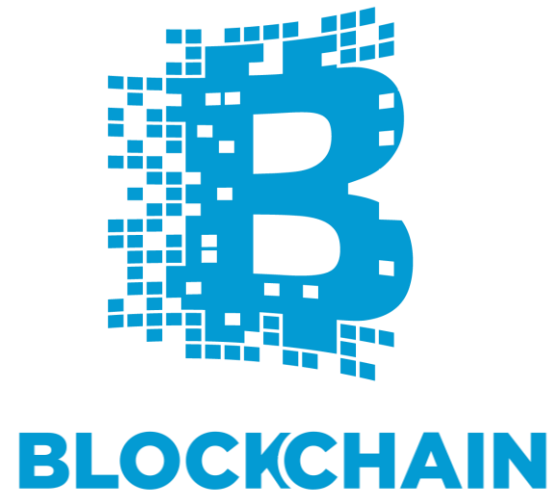
블록체인 원리

수수료 및 BTC발행을
보상으로 경쟁적
채굴을 유도하고,

이를 통해 시스템의
신뢰도를 확보한다!



블록체인 원리



블록체인 응용



BLOCKCHAIN

블록체인은 비트코인에만 적용될 수 있는것이 아니다!

블록체인은 비트코인을 상용화 가능하게 만든 하나의 시스템일뿐

블록체인의 일반화

사람들간의 '약속'을 제3자의 개입 없이도 신뢰할 수 있도록 보장해주는 시스템

신뢰는 어디에서 오는가?

'약속'의 위변조가 불가능함. '약속'이 사라지지 않고 영구적으로 저장
이전에 설명했던 블록체인의 기술적 특징이 이를 보장한다!

블록체인 응용



투표시스템

투표도 하나의 '약속'

현재는 감사기관 및 중앙관리기관에 의해
그 신뢰성을 보장하고 있으나, 완벽하지 않다!

블록체인으로 '투표기록'을 관리!

블록체인 응용



투표시스템

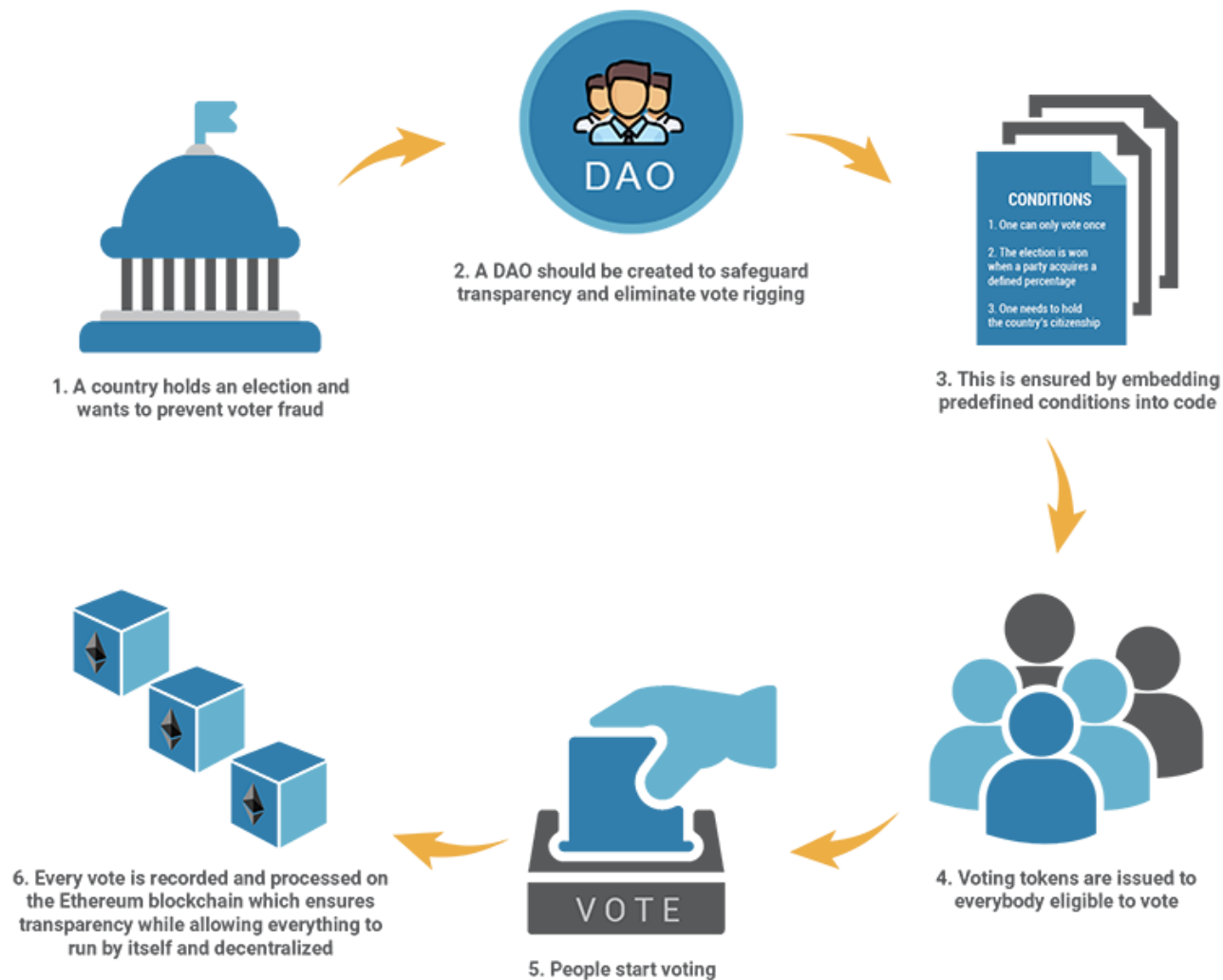
투표도 하나의 '약속'

현재는 감사기관 및 중앙관리기관에 의해
그 신뢰성을 보장하고 있으나, 완벽하지 않다!

블록체인으로 '투표기록'을 관리!

이와 같이 기존시스템을 탈중앙화된 app
으로 만든것을 **dApp** (decentralized application)
이라 한다.

블록체인 응용



블록체인 응용



스마트 컨트랙트

특정 조건을 만족하면 자동적으로 계약내용을 실행하도록 하는 온라인상의 계약서

계약의 변조가 불가능하여야 하고,
영구히 그 기록이 보존될 수 있어야 한다!

블록체인 응용



스마트 컨트랙트

특정 조건을 만족하면 자동적으로 계약내용을 실행하도록 하는 온라인상의 계약서

계약의 변조가 불가능하여야 하고,
영구히 그 기록이 보존될 수 있어야 한다!

비트코인의 블록체인 시스템에서 사용가능한 계약 스크립트: "a가 b에게 xxxBTC를 보낸다"

if, else 등의 조건문과 **for loop** 등의 반복문을 사용하여 계약을 더 다양하게 기술할 수 있게 만든다면!
→ **스마트 컨트랙트의 실현!**

블록체인 응용



ethereum

이더리움 플랫폼은 자체언어를 이용하여
if, else 등의 조건문과 for loop 등 반복문을 통해
임의의 논리를 포함하는 계약을 가능하게 하였다.
-> **'튜링완전하다'**

이더리움 플랫폼을 이용한다면,
블록체인 시스템을 처음부터 개발하지 않더라도,
이전에 설명하였던 **dApp** 들을 손쉽게 개발할 수 있다!

블록체인 응용



ethereum

이더리움은 'Ether' 이라는 화폐단위를 쓰며
dApp을 만들기 위해 스크립트를 짜는 사람들에게,
스크립트 복잡도에 비례하는 Ether 과금을 한다.

이더리움은 가상화폐의 발행처인 동시에,
이의 소비처이기도 하다.

블록체인 응용



저작권

저작권과 같은 지식재산권도
블록체인을 통해서 관리할 수 있다!

저작권협회 등 3자의 관리 없이도
더욱 투명하고 안전하게 관리 가능!

더불어, **스마트 컨트랙트** 기능을 사용한다면,
각 저작권에 해당되는 저작권료 지불 등의
거래가 자동적으로 수행되게 할 수 있다!

이더리움 플랫폼 기반으로, 저작권 관련
dApp들이 많이 개발되고 있다!

블록체인 응용



1. Rights holder publish ownership information on the blockchain



2. Use policies for registered works are written into smart contracts that automatically transfer usage rights



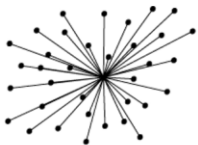

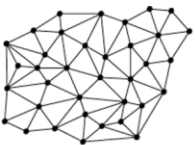




























3. Royalties and fees are delivered instantly, transparently and automatically based on the stakeholder information contained in the blockchain database



4. An open platform facilitates infinite potential roles, applications and business models

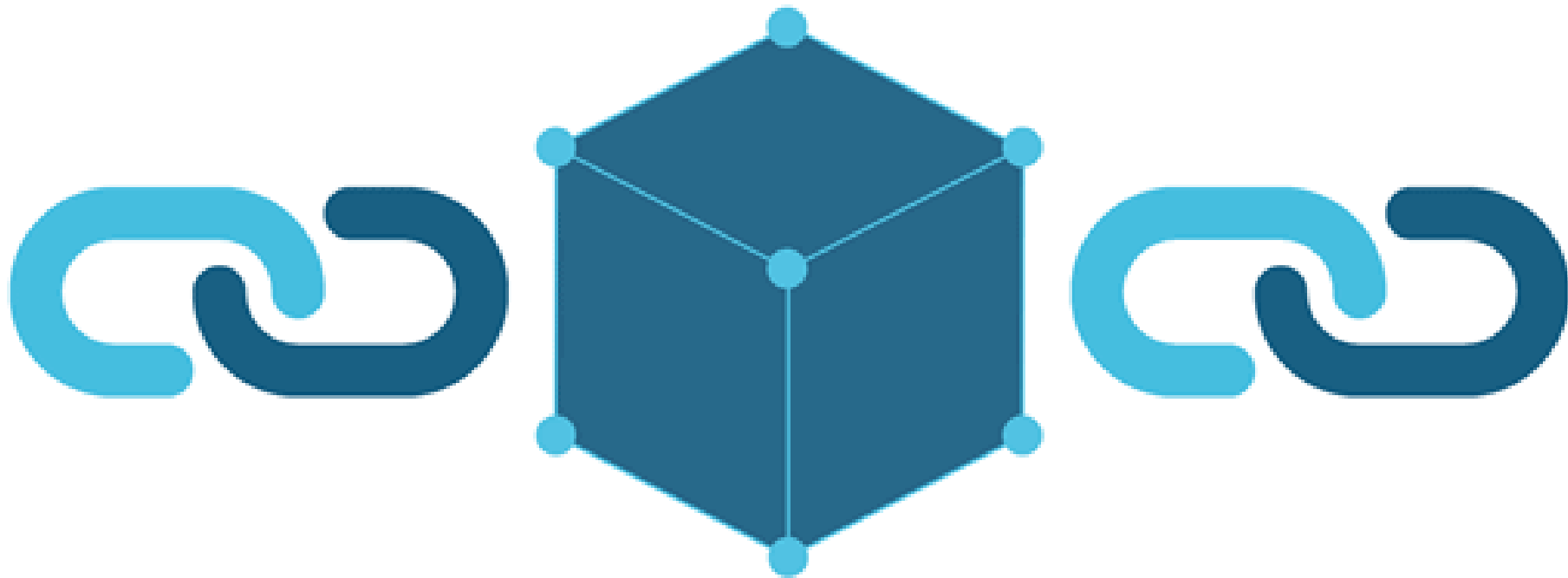
블록체인 응용

블록체인의 더욱 다양한 응용 사례 및 관련 스타트업

 PAST	 PRESENT	 FUTURE	<h3>Blockchain Startups</h3> <p>Top Blockchain startups disrupting non-financial markets</p>  Venture Radar
 THE WALL STREET JOURNAL THE TIMES HM Government Hilton	 facebook twitter Dropbox UBER airbnb	 Social Networking  synereo  GEMS Digital Identity  ONENAME  ShoCard Art & Ownership VERISART  Bitproof.io  MONEGRAPH  colu.	<p>Cloud storage  Filecoin  STORJ.IO  TIERION</p> <p>Smart Contracts  TRUST  EP ETHERPARTY  appliedblockchain</p> <p>Anti-Counterfeiting  everledger  BLOCKVERIFY</p> <p>Governance  OTONOMOS  Swarm  followmyvote  BITNATION GOVERNANCE 2.0</p> <p>Supply Chain  thingchain  Tradle</p> <p>Prediction Markets  augur</p> <p>Internet of Things  FILAMENT </p> <p>More: https://www.ventureradar.com/</p>

블록체인 응용

우리는 블록체인 기술을 활용하여 무엇을 바꿀 수 있을까?



중앙집중적인 사고방식에서 벗어나, 더욱 더 투명하고 안전한 세상을 만들 수 있는 첫걸음!



Question

The End