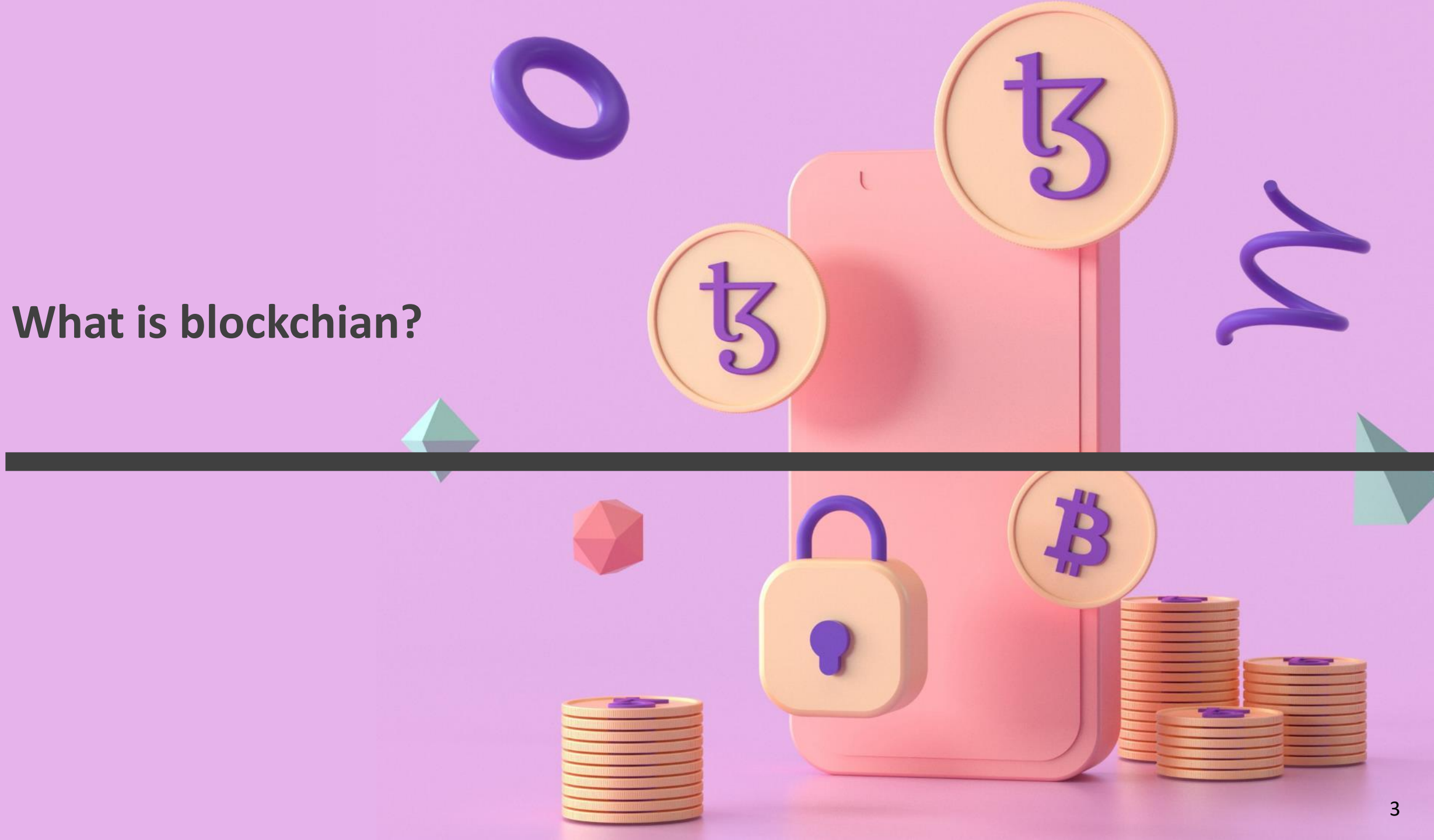
S_C_P 김원태

BLOCKCHAIN & Bitcoin

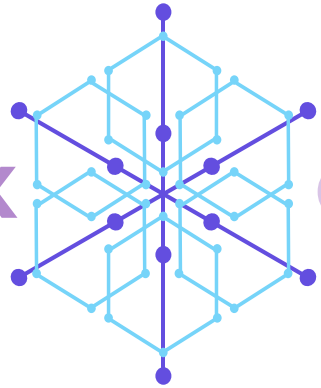
목차

What is blockchian?



Part 1

블록체인은 무엇인가?

[BLOCK  CHAIN ≠ bitcoin]

블록체인이란??

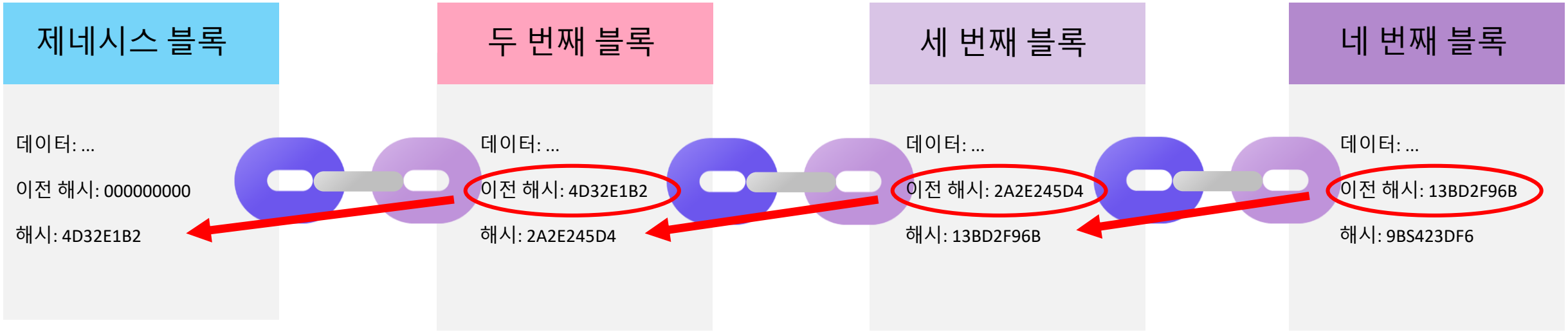
Part 1

블록체인은 무엇인가?

1. 데이터 : “안녕”
2. 이전 해시 : 00000000
3. 해시 : 4D32E1B2

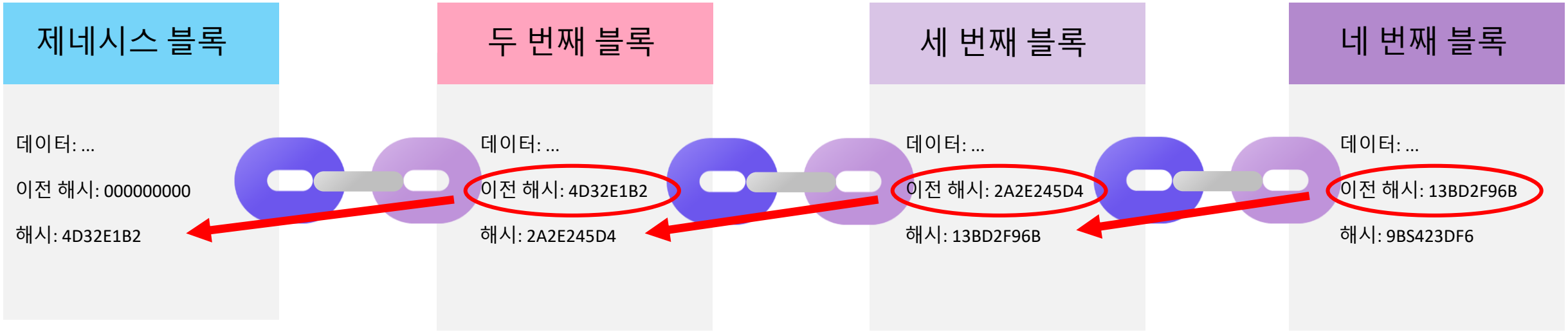
Part 1

블록체인은 무엇인가?

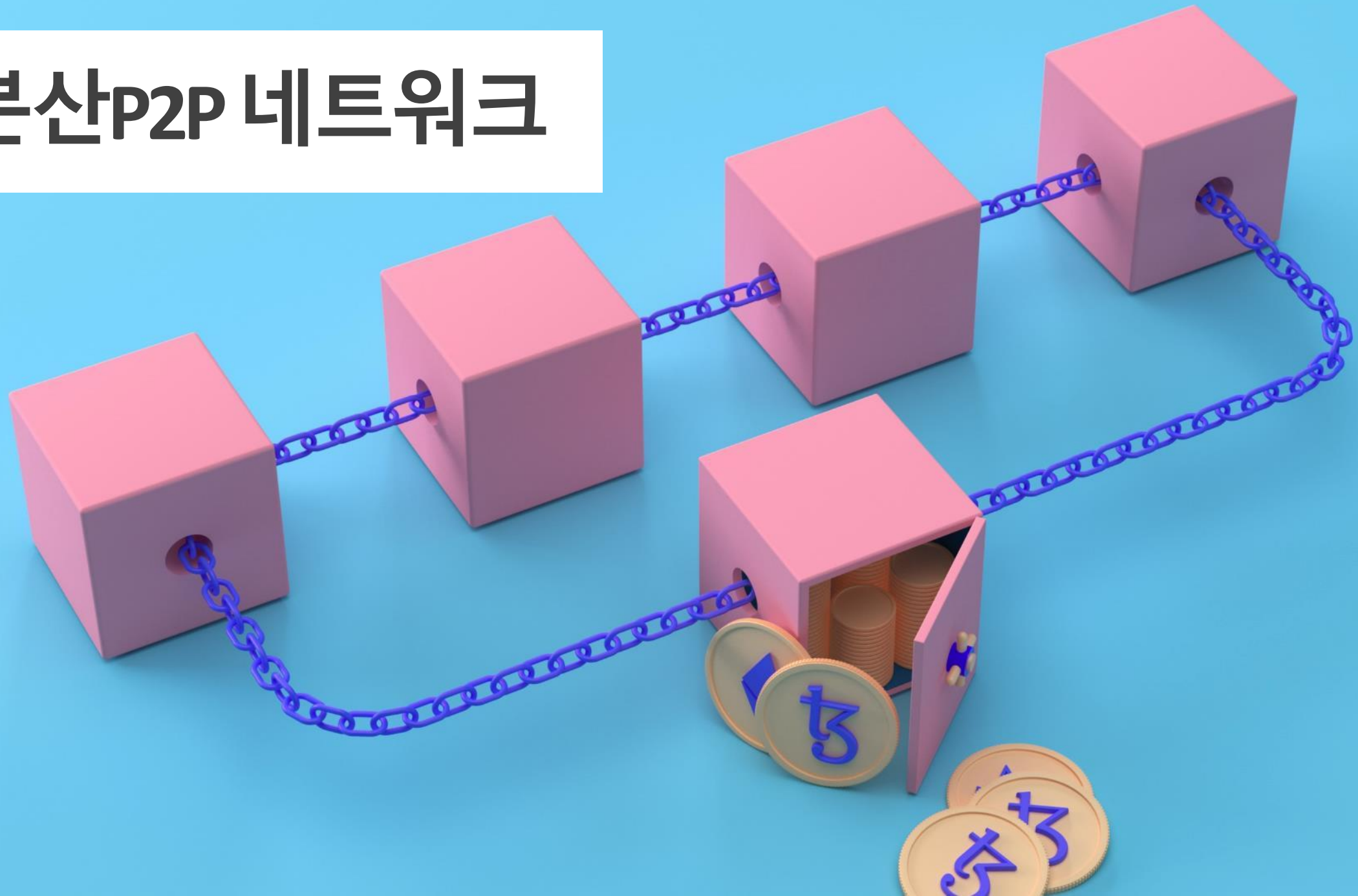


Part 1

블록체인은 무엇인가?



#분산P2P 네트워크



Part 2

분산 P2P 네트워크??

분산 P2P 네트워크??

2a89bf1700a9140aa496380fd0b4443921bbeefb9cdb9ef
6ea7404cf82286afc

SHA256
(Secure Hash Algorithm)

256비트의 고정된 결과값을 출력하며 64자리의 길이를 가진 16진법 문자열 형태로 나타냅니다. 미국 국가안보국 NSA에서 개발된 알고리즘으로 비트코인 외 다양한 분야에서도 사용되고 있습니다.

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C ,D ,E, F

Part 2

분산 P2P 네트워크??

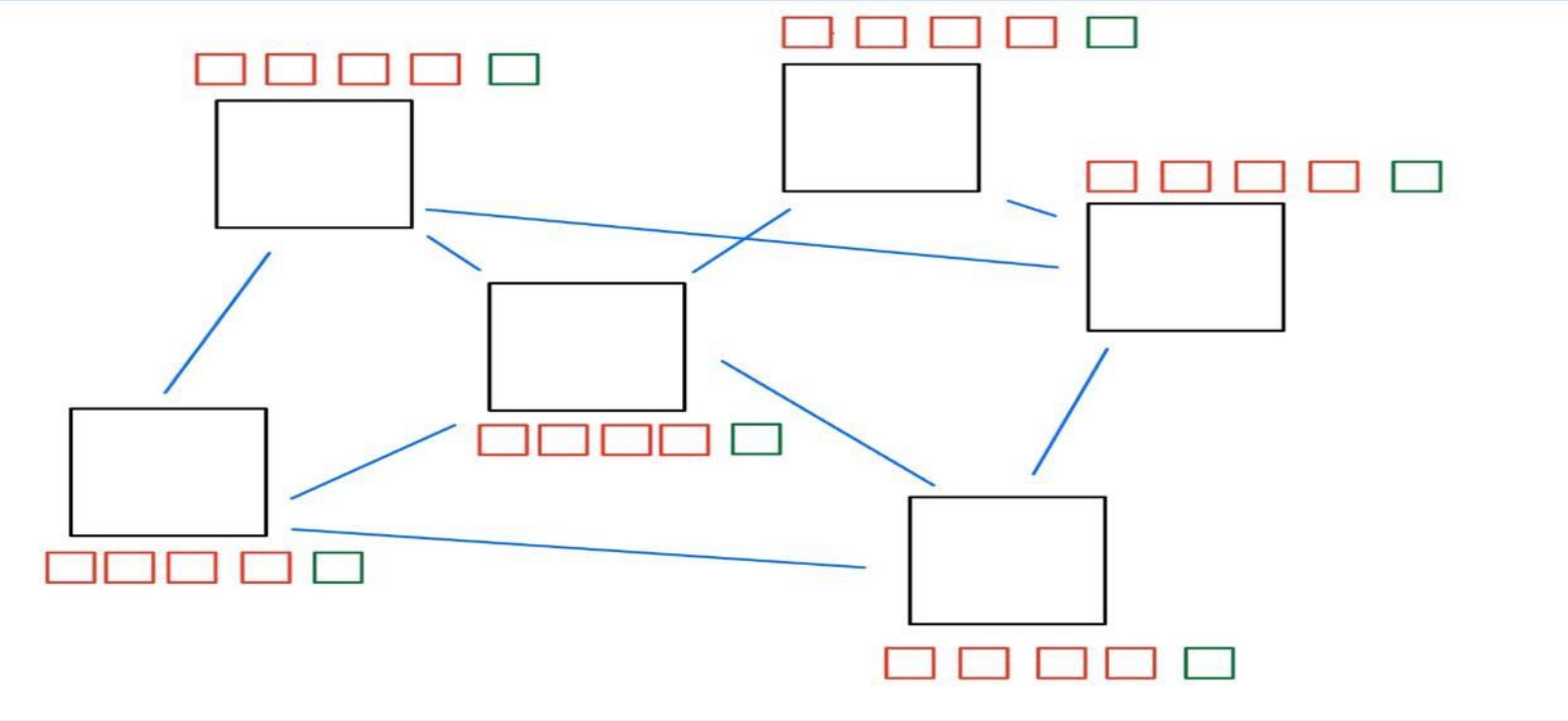
https://tools.superdatascience.com/blockchain/hash

해시 알고리즘의 5가지 요구사항	
단방향	해시를 재구성할 수 없어야 합니다. 재구성이 목적이 아닌 식별이 목적이며 암호화용이 아닌 문서 식별이 목적이기 때문입니다.
결정록적 알고리즘	문서를 가져가서 몇 번의 알고리즘을 적용하더라도 매번 같은 결과를 얻어야 합니다.
신속한 계산	매우 빠르게, 거의 즉각적으로 계산이 되어야합니다. 데이터가 변할 때 즉시 바뀌어야 하기 때문입니다.
쇄도 효과	"."이라는 아주 작은 값을 변경해도 해시값은 완전히 바뀌게 됩니다. 이는 예측 가능성이라는 문제를 해결하는 데 도움이 됩니다. 또 어떤 해시, 어떤 문서를 갖게 될지 알 수 없으므로 문서와 해시 사이의 연결고리를 끊어 보안을 유지해줍니다.
충돌 저항성	충돌은 해시함수의 결과 값이 동일하다는 말입니다. 동일한 해시를 가지는 서로 다른 2개의 데이터 세트를 생성해보기는 매우 힘듭니다. 생성하지 않은 것을 추측하는 것도 거의 불가능하고 추측하려면 엄청난 시간과 노력이 필요합니다. 그래서 충돌을 잘 견뎌야 합니다.

Part 2

분산 P2P 네트워크??

제가 공부한 블록체인에서 P2P는 (peer-to-peer)
하나의 블록체인이 중앙 집중된 위치에 하나의 블록체인의 사본이 있다고 가정하고 이 동일한 복사본이 네트워크 상의 모든 컴퓨터에 복사되어 존재하고 재산의 거래가 중앙 집중된 위치에서 기록되면 클론에게도 모두 기록이 됩니다. 시간이 지나 블록들이 더욱 쌓이게 되었고 해커가 공격을 통해 초록색 블록을 공격하고 뒤이어 생겨있던 블록들도 위조해서 괜찮은 것처럼 보이게 합니다. 하지만 연결되어 있는 모든 컴퓨터에 복사본이 저장되어 있고 이상을 감지하게 됩니다. 이 문제를 감지하면 올바른 복사본으로 다시 되돌려둡니다.



Part 3

비트코인 & 채굴

Part 3

비트코인&채굴

빗썸

비트코인 BTC

39,673,000원

▲456,000 +1.16% | 한국 프리미엄 +0.09%

05.01. • 실시간

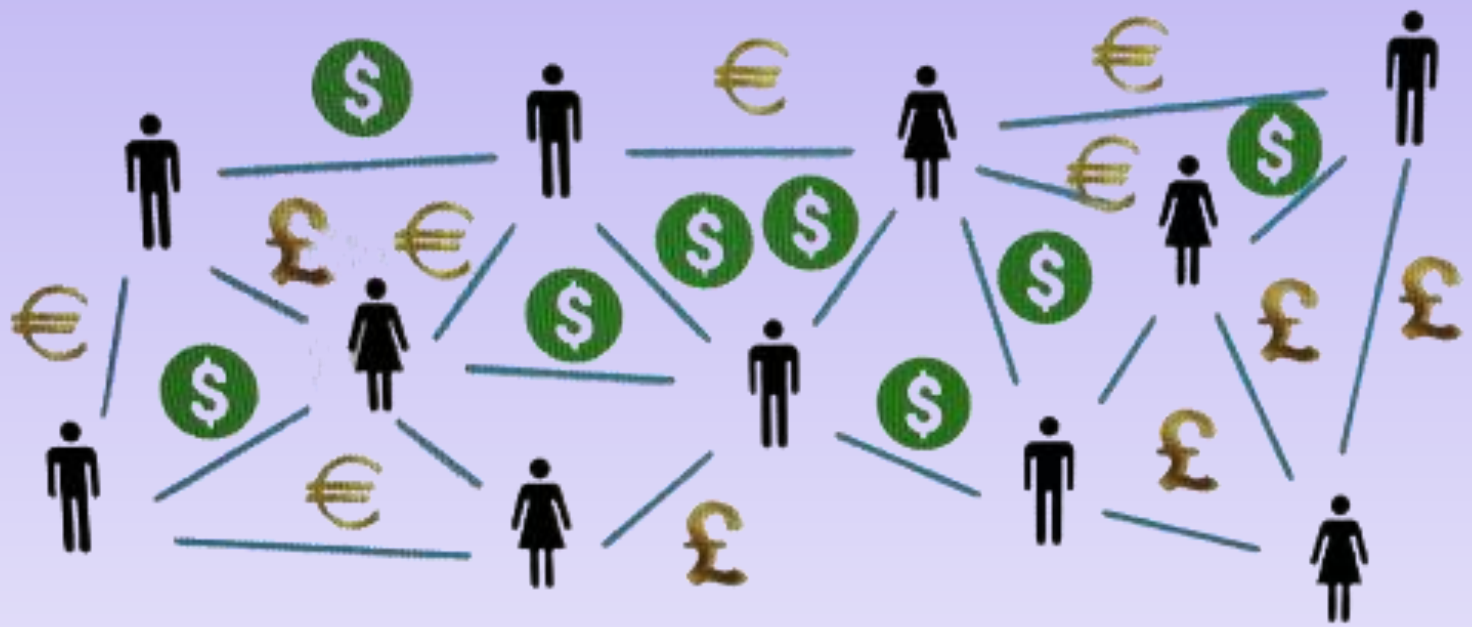
1일 1주 1달 3달 1년

전일	39,217,000	시가	39,219,000	고가	39,742,000	거래량	916.807 BTC
저가	39,217,000	거래대금	358억				

52주 최저 • 최고

20,743,000 — 50,996,000

사토시 나카모토가 2008년에 처음 소개했으며
현재까지도 이 사람이 누구인지 밝혀진 게 없습니다.



비트코인 네트워크에 참여하는 컴퓨터들이 서로 검증하고 공유하는 거래 정보를 블록체인에 기록하고
이러한 거래 정보를 블록체인에 기록함으로써, 중앙기관 없이도 거래의 신뢰성을 보장할 수 있습니다.
더욱이 비트코인을 해킹하려면 블록체인에 기록된 모든 정보를 동시에 조작해야하므로 사실상 불가능에 가깝습니다.

[ ]

블록체인과 비트코인을 공부하며 느낀점
&
다음으로 공부할 것

감사합니다