

블록체인은 왜 ‘블록체인’ 일까 ?

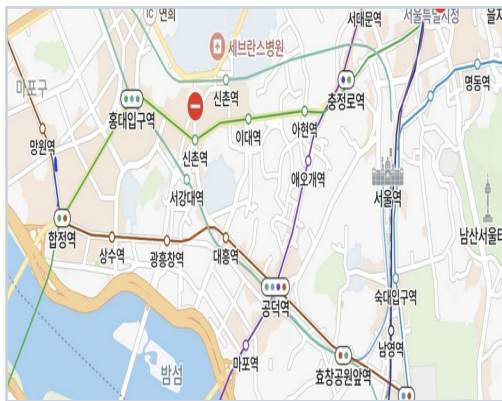
왜 Block 인가 ? 왜 Chain 인가 ? 왜 Distributed 인가 ?

김동규 · 서강대학교 블록체인 과정 이전 기수 강의

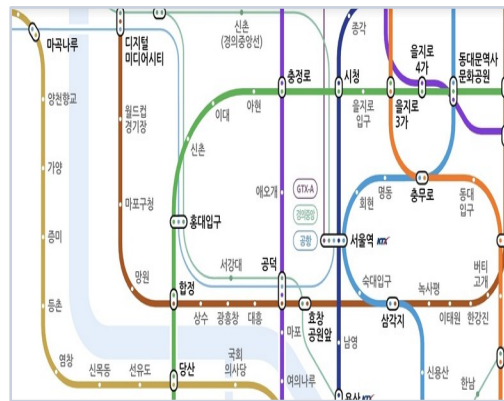
오늘은 조금 단순하게 설명하겠습니다

물은 100°C 에서
끓는다

“항상?”



실제 지도



지하철 노선도

오늘의 목표는 위성사진이 아니라 ‘블록체인 지하철 노선도’ 를 만드는 것입니다 .

장부에 대한 믿음은 어디에서 오는가 ?

왜 은행 장부의 100 만원은 믿을까 ?

은행 장부

잔액 1,000,000 원



왜 왼쪽은 믿고
오른쪽은 믿지 않을까 ?

내 노트

잔액 2,000,000 원

중앙화된 장부 = 공식 장부를 관리하고 최종 판단하는 주체가 있다



“이게 공식 장부입니다” 라고
한 사람이 말할 수 없다면 ?

1 기록이 바뀌지는 않았는가 ?

Hash

2 기록을 어떻게 묶을까 ?

Block

3 과거와 현재를 어떻게 연결할까 ?

Chain

4 여러 참여자가 같은 장부를 어떻게 공유할까 ?

Distributed Ledger

5 서로 다르면 무엇을 진짜라고 할까 ?

Consensus

Hash



Block



Chain



Distributed Ledger

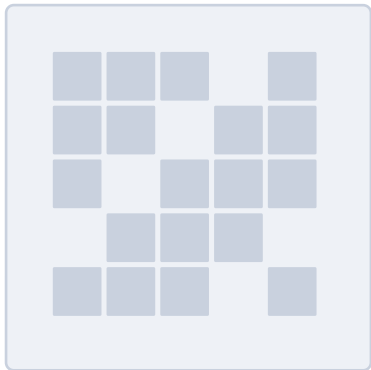


Consensus



Hash — 기록의 지문

첫 번째 실습 · 스마트폰으로 QR 을 스캔해 직접 해시를 계산해 보세요



QR 코드 삽입
(해시 계산 사이트)

철수가 영희에게 10000 원을 보냄

숫자 하나만 바꾸면 ?

철수가 영희에게 1000**1** 원을 보냄

HASH → ?

HASH → ?

Hash = 데이터의 디지털 지문

“오늘은 이렇게 이해하겠습니다.” · 암호화 (숨기기) 가 아니라 변경 확인용 지문



Hash



Block



Chain



Distributed Ledger



Consensus



PoW



Ethereum

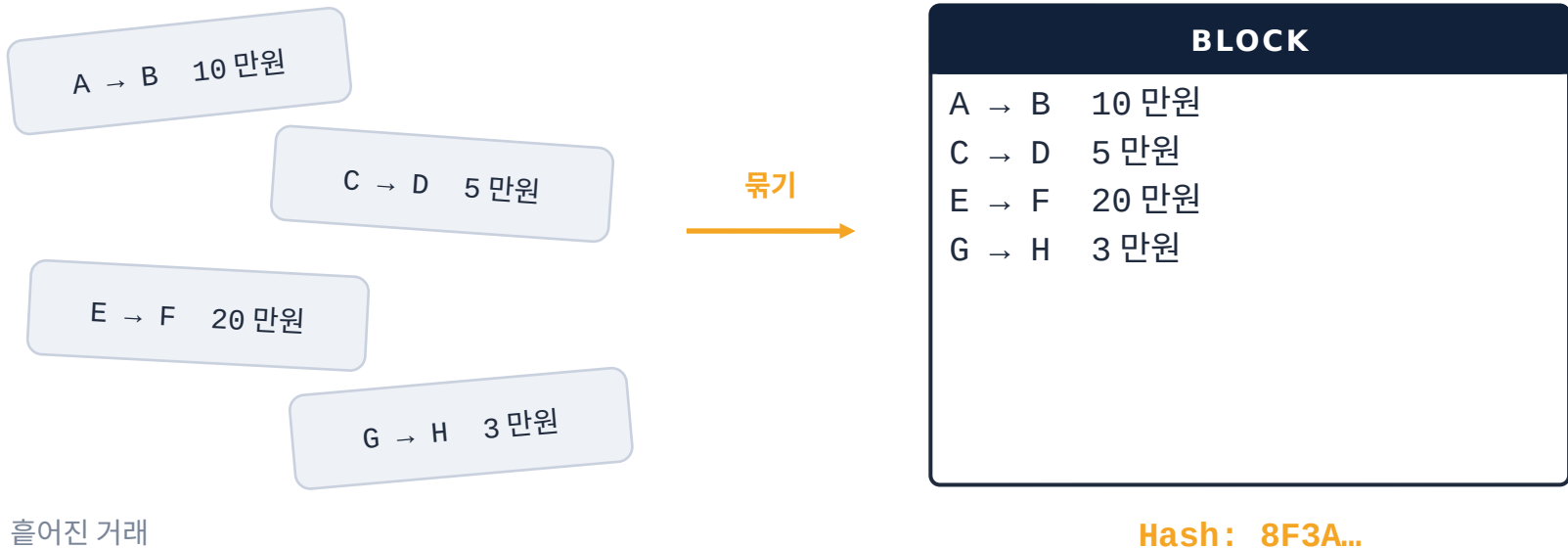


Smart Contract



DApp

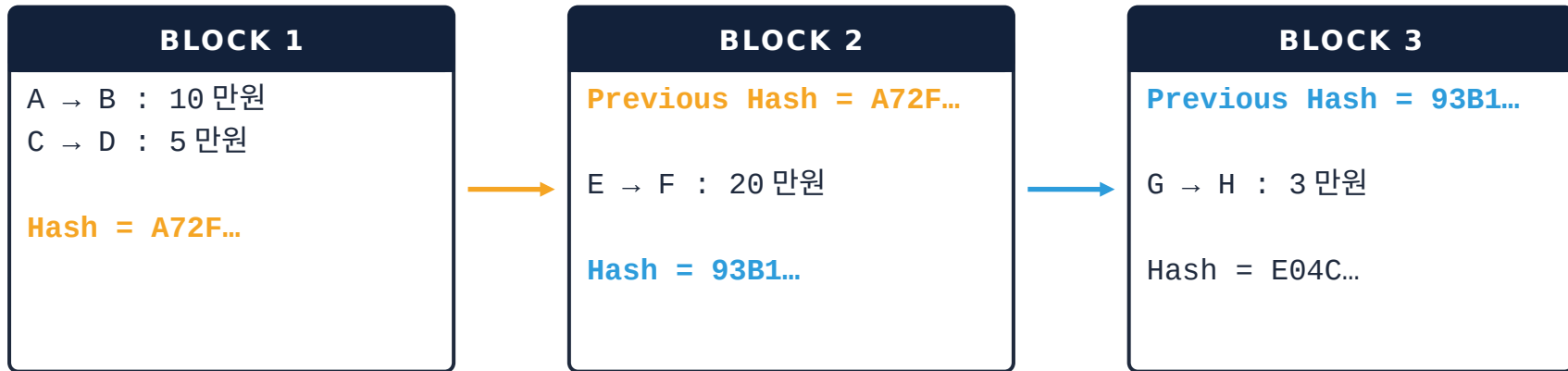
왜 Block 일까 ?



여러 기록을 일정한 단위로 묶는다



왜 Chain 일까 ?

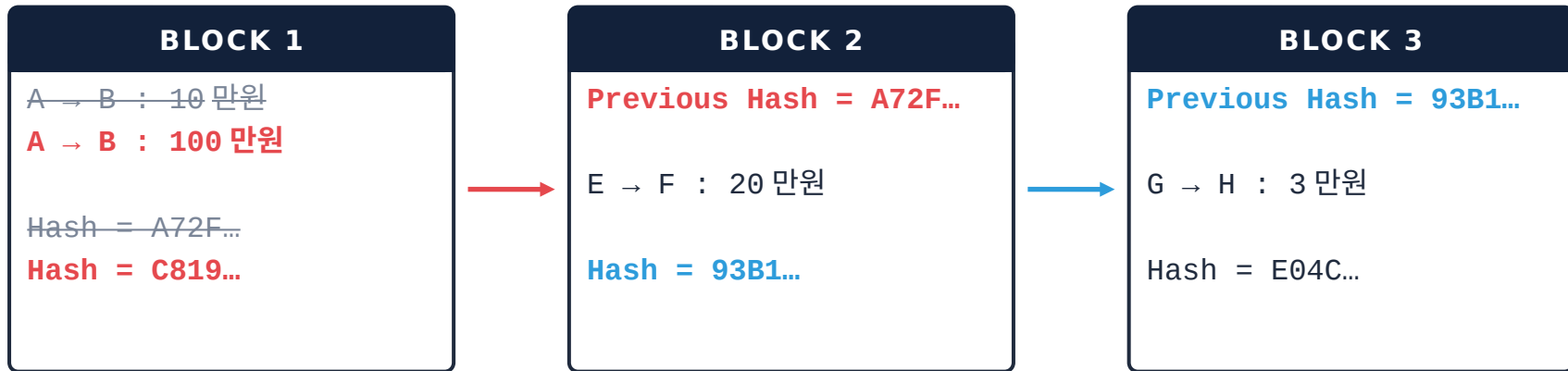


같은 값 → 앞뒤가 연결된다

다음 Block 이 이전 Block 의 Hash 를 기억한다



하나를 바꾸면 ?



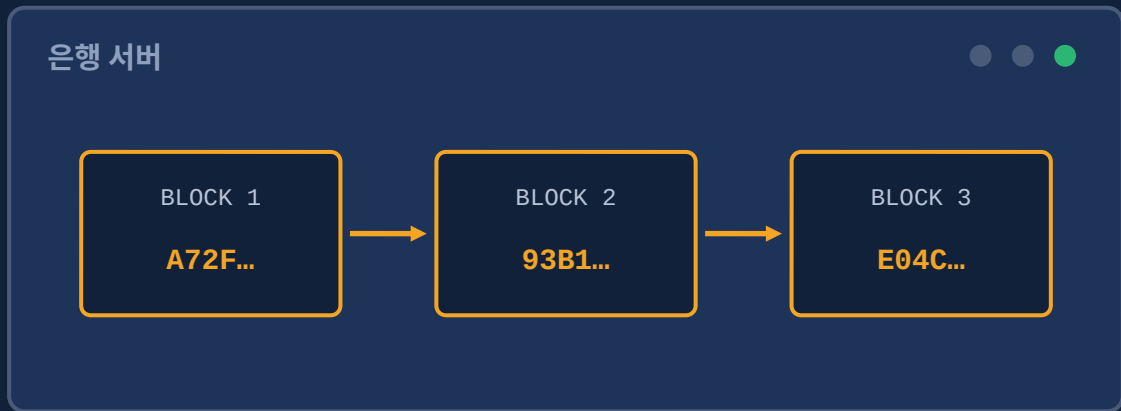
× Mismatch

C819... ≠ A72F...

바꿀 수 없는 것이 아니라 , 바꾸면 연결이 깨진다

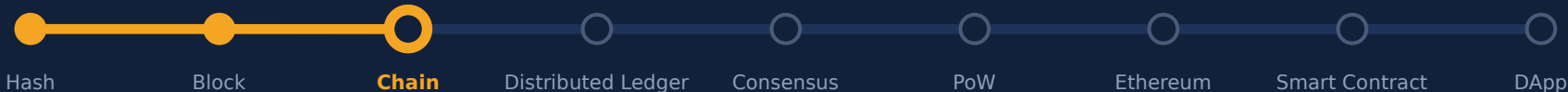


그런데 여기까지만이라면 ?



“ 이것도 은행 서버에서 만들 수 있지 않을까 ? ”

다시 질문 : 누가 이 장부를 가지고 , 누가 공식 기록을 결정하는가 ?



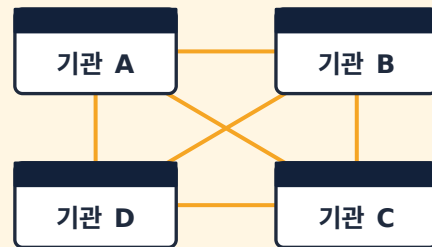
서버가 여러 대면 분산원장일까 ?

분산된 서버



관리자 = 은행

분산원장



공통 규칙으로 보유 · 검증 · 인정

서버가 어디에 있는가 ≠ 누가 장부를 결정하는가



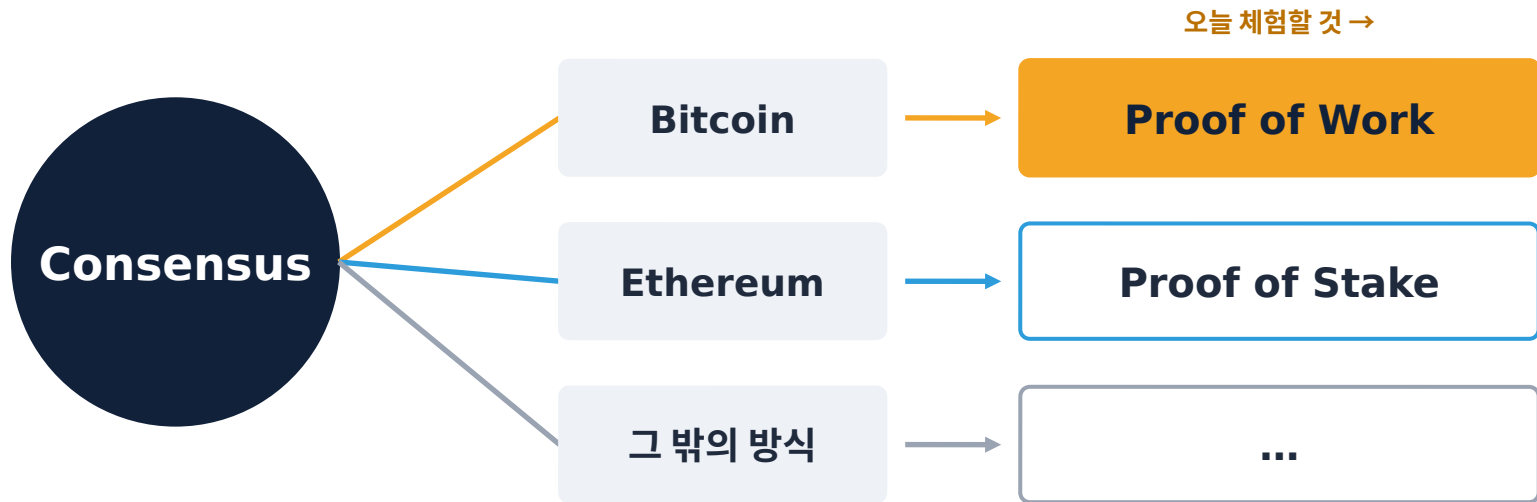
장부가 서로 다르다면 ?



한 참여자가 단독으로 정답을 선언하지 않는다면, 공통 규칙이 필요하다



Consensus에는 여러 방법이 있습니다



이제 다시 스마트폰을 꺼내주세요 .



‘00’ 을 먼저 찾아라



QR 코드 삽입 (해시 사이트)



Blockchain 1
→ Blockchain 2
Blockchain 3
...

Hash 앞 두 자리가 00 인 숫자를 먼저 찾으세요 .

먼저 찾은 사람은 손을 들어 주세요 . “ 설명하지 않을 테니 일단 해보겠습니다 .”



방금 ‘어려운 수학문제’ 를 풀었을까 ?

채굴 = 어려운 수학문제를 푼다 ?

A

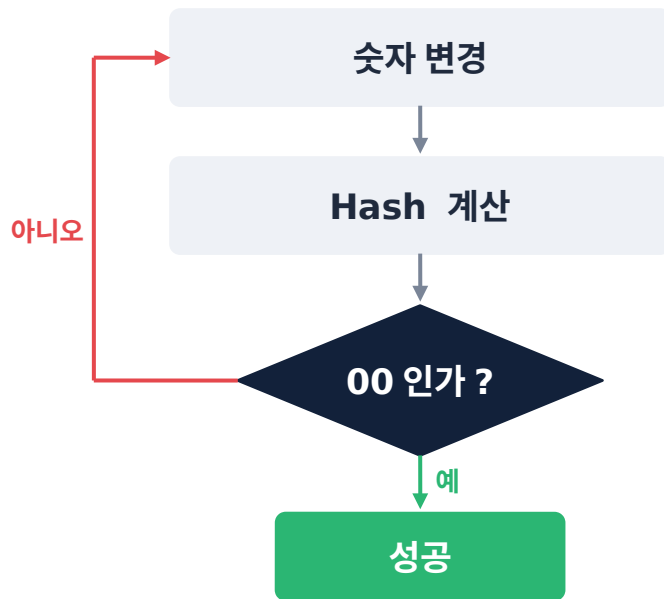
초당 10 회

B

초당 1,000,000 회

누가 먼저 찾을 가능성이 높을까 ?

실제 Bitcoin 에서는 ‘00’ 의 개수가 아니라 Hash 가 Target 보다 작은지를 판단



조건을 만족할 때까지 반복해서 시도한다



그래서 먼저 찾으면 무엇을 하나 ?

“00 을 찾았습니다. 그래서요?”

성공 !

NEW BLOCK

Hash = 00A7...

Prev = E04C...

B

“ 이 Block 을 다음 Block 으로
제안합니다 .”

A

a1c7...
계산 중...

B

C

f09e...
계산 중...

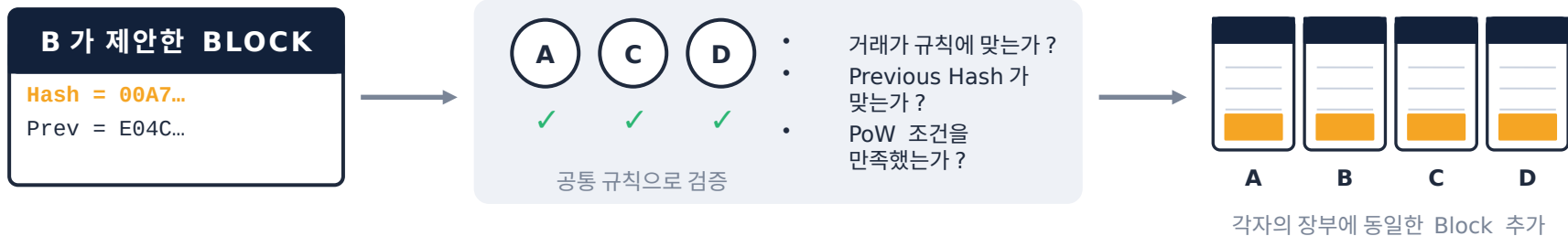
D

7b22...
계산 중...

PoW → 다음 Block 을 ‘제안’ 할 기회와 연결



제안했다고 끝이 아니다



제안 ≠ 인정



먼저 찾았다고 마음대로 장부를 쓸 수 없다 · 다른 노드가 공통 규칙으로 검증한다



장부에 대한 믿음은 어디에서 올까 ?

중앙화된 장부

관리주체가 공식 장부를 결정

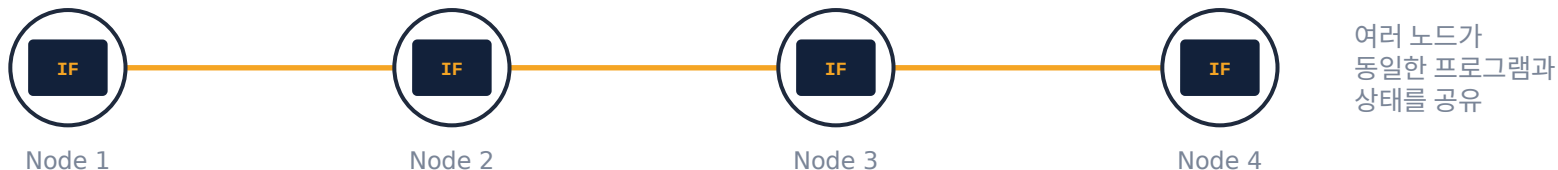
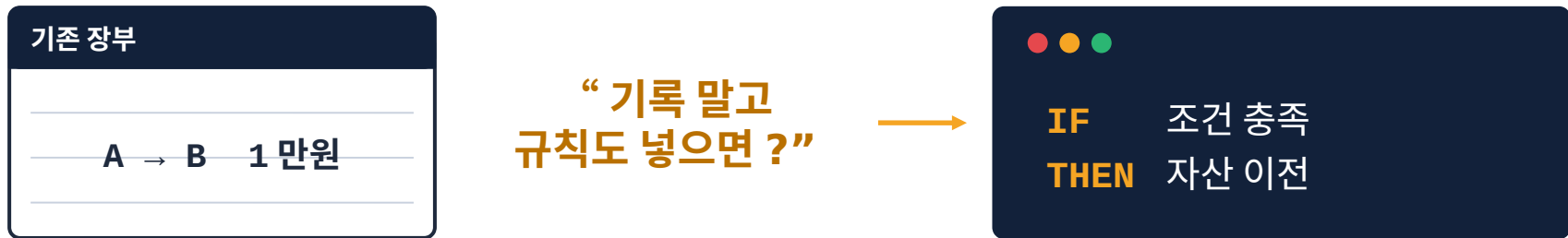
분산원장

공통 규칙에 따라 보유 · 검증 · 합의



“ 이 장부에는 송금 기록만 적어야 할까 ? ”

Ethereum 은 왜 World Computer 라고 할까 ?

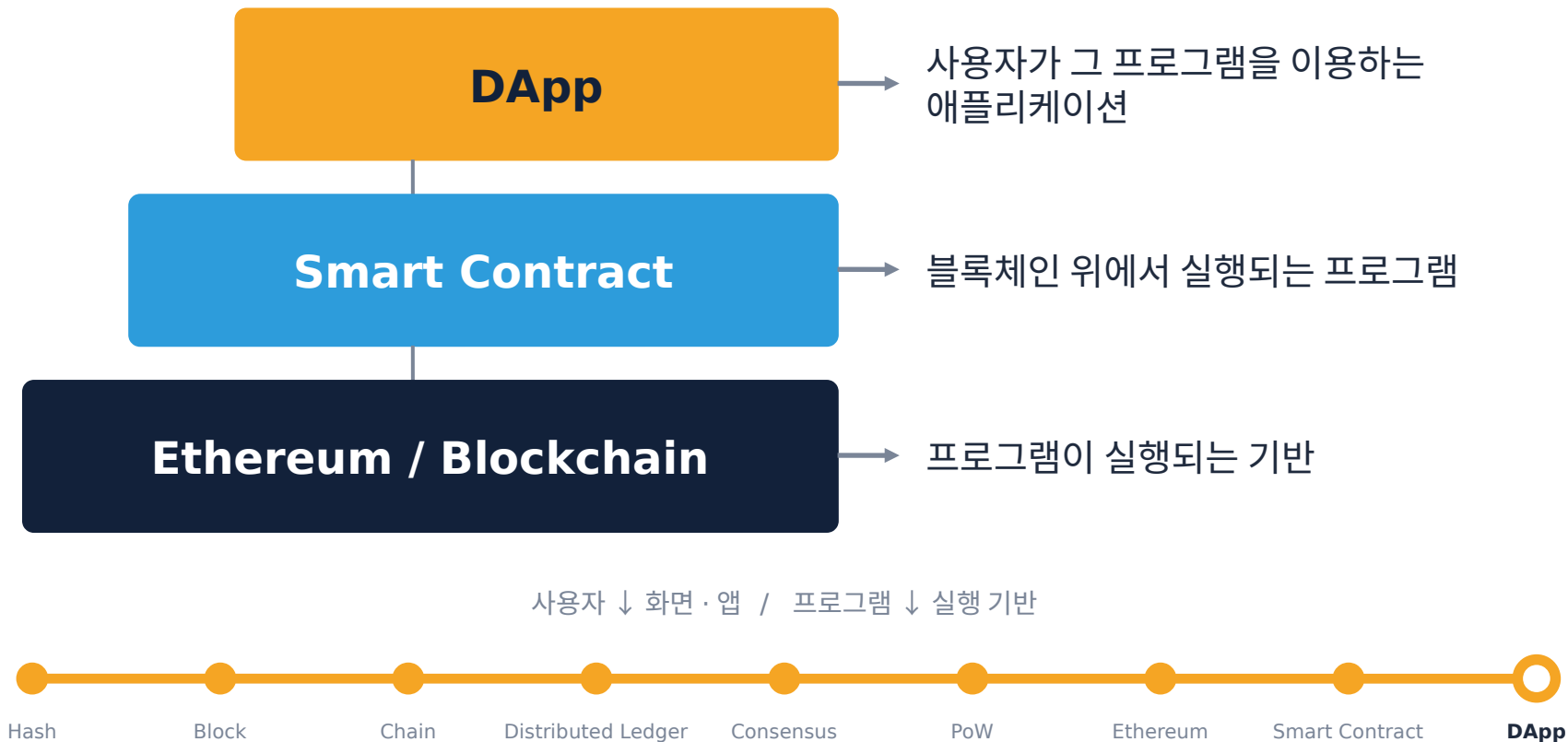


World Computer

“한 대의 거대한 컴퓨터라는 뜻은 아니다.”



Smart Contract 와 DApp



오늘 만든 블록체인의 노선도



- 왜 **Block?**

기록을 묶기 위해

- 왜 **Chain?**

기록을 연결하기 위해

- 왜 **Distributed?**

한 중앙 장부에만 의존하지 않고 여러 참여자가 보유 · 검증하기 위해

- 왜 **Consensus?**

무엇을 올바른 기록으로 인정할지 결정하기 위해

- 왜 **PoW**에 컴퓨팅 파워가 필요한가?

조건을 만족하는 값을 찾기 위해 반복 계산하기 때문에

- **Smart Contract?**

블록체인 위에서 실행되는 프로그램

- **DApp?**

그 프로그램을 사용하는 애플리케이션



오늘 만든 것은 블록체인의 ‘지하철 노선도’ 입니다 .

Bitcoin · Ethereum · Stablecoin · NFT · STO · RWA · DeFi · CBDC · Web3 ...

새로운 개념이 나오면 , 오늘 만든 노선도의 어디에 있는 이야기인지 먼저 생각해 보세요 .