SDF데이터클래스

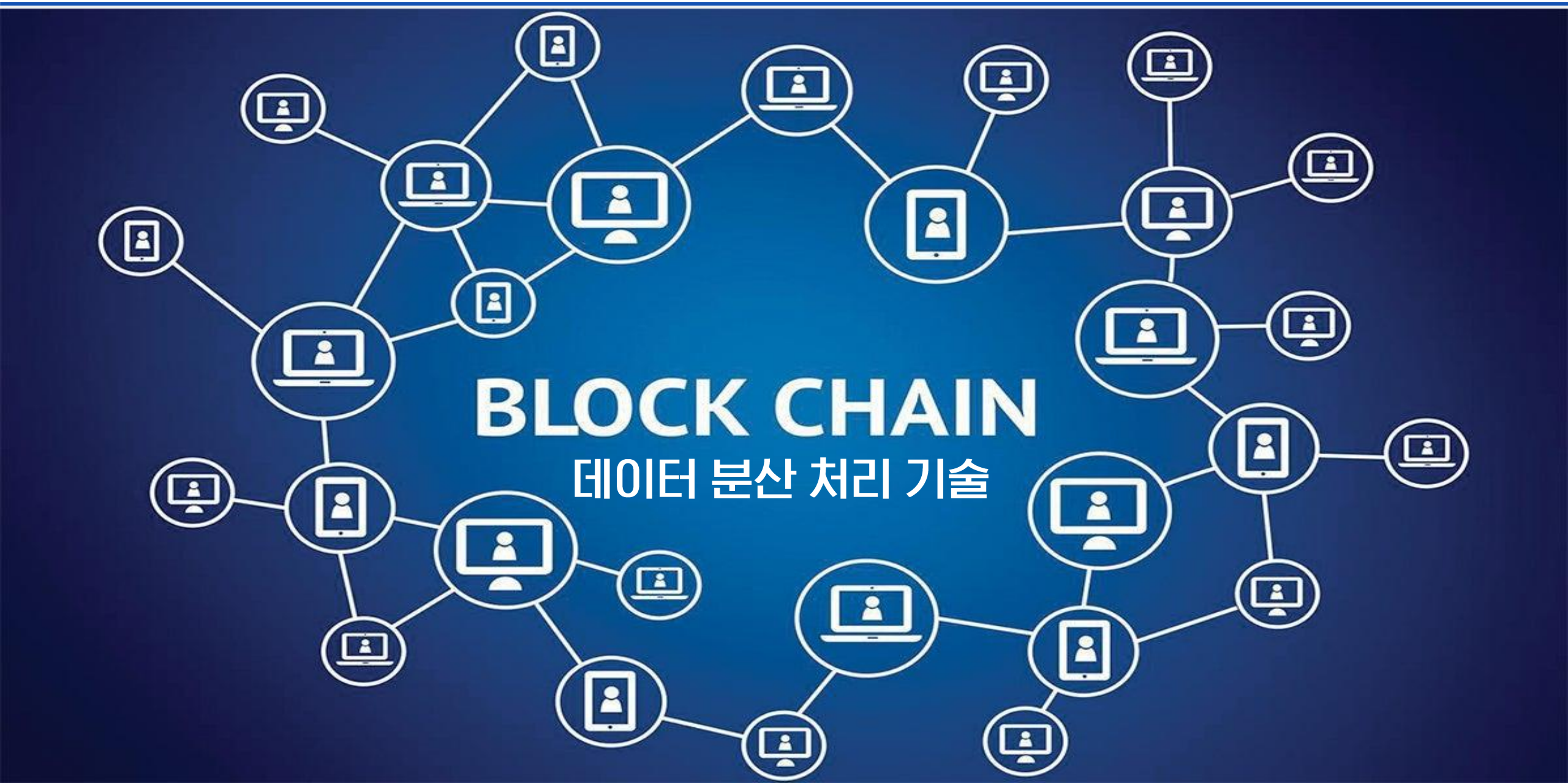
디지털트렌드 교육

#2. 블록체인

Seoul Digital Foundation
서울디지털재단

블록체인은 무엇인가?

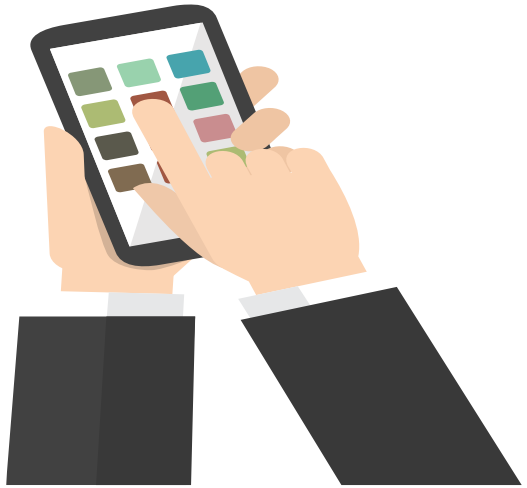
블록체인은 무엇인가?



왜 분산 처리해야하는가?

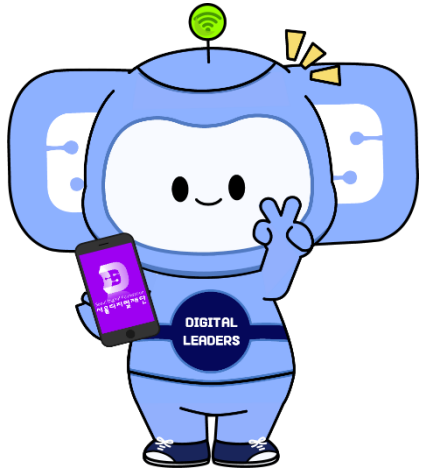
기존 인터넷 뱅킹으로 송금하면 벌어지는 일

① "월디"에게 만원을 보내야지~
인터넷뱅킹에서 "송금 1만원" 클릭



② A의 통장 잔고가 얼마지?
오~ 만원이 있구만…
그럼 A의 잔고에서 만원을 빼서
월디에게 보내야지!

③ 월디통장에 만원 입금 (거래종료)



거래의 증거는 은행장부에 적힌 "A의 출금 기록 " 및 "월디 입금 기록"

왜 분산 처리해야하는가?

거래의 유일한 증거인 " 은행장부 " 가 삭제되거나, 공격당한다면?

이러면 안되기 때문에…
모든 은행은 장부의 기록을 최대한의 노력으로 숨기려 노력하고 철통보안을 유지하려 하지만 근원적 해결이 될 수 없다!

[금융권 사이버 공격史] NH농협부터 카카오·신한은행까지 줄수난

강진규 기자 | 입력 2020.08.28 08:00 | 수정 2020.08.28 09:14 | 댓글 0

최근 은행, 한국거래소 디도스 공격에 과거 악몽 떠올리는 금융권
인터넷뱅킹 마비, 정보유출, 데이터 손실 등 각종 사고로 몸살

2009년부터 최근까지 금융권은 해킹 공격으로 큰 피해를 입고 있다. [사진: 셔터스톡]

검색어

Digital Today TV Live
NGINX 마이크로서비스
엔진엑스와 함께
무한 가능성의 세

인기기사

1 해외 가상자산 거래소 국내서 꼼수
2 이더리움, 17일 세폴리아 테스트
3 '선 넘지 말라'... 융당국, 앱 편의성
4 글로벌 빅클라우드, 한국 공공 시

△밥 모리츠 PwC 회장

"사이버 리스크에 가장 취약한 곳은 디지털화(digitalization)가 가장 많이 일어난 곳, 바로 금융권이다."

밥 모리츠 프라이스워터하우스쿠퍼스(PwC) 회장은 17일 매일경제와의 단독 화상 인터뷰에서 이같이 밝혔다. 이날 PwC가 발표한 '2022년 글로벌 최고경영자(CEO) 설문조사'에서 최대 글로벌 위협 요인으로 사이버 리스크가 꼽혔는데, 여기에 가장 영향을 많이 받는 곳이 금융이며 이에 대한 보안책 마련이 필요하다는 설명이다. 모리츠 회장은 "코로나 기간에 은행, 핀테크 등 금융권이 디지털 부문에서 가장 많은 변화를 일으켰다"며 "지난해 금융권에서 다뤄지는 온라인 데이터 양이 기하급수적으로 늘었고, 그 와중에 랜섬웨어(악성 프로그램) 같은 사이버 공격도 그만큼 많이 일어났다"고 밝혔다.

그는 또 "복잡한 금융 시스템이 해킹으로 한 군데라도 뚫리면 전체 시장이 뒤흔들릴 수 있다"고 경고했다.

기존의 문제를 역으로 해결하려는 블록체인의 시도

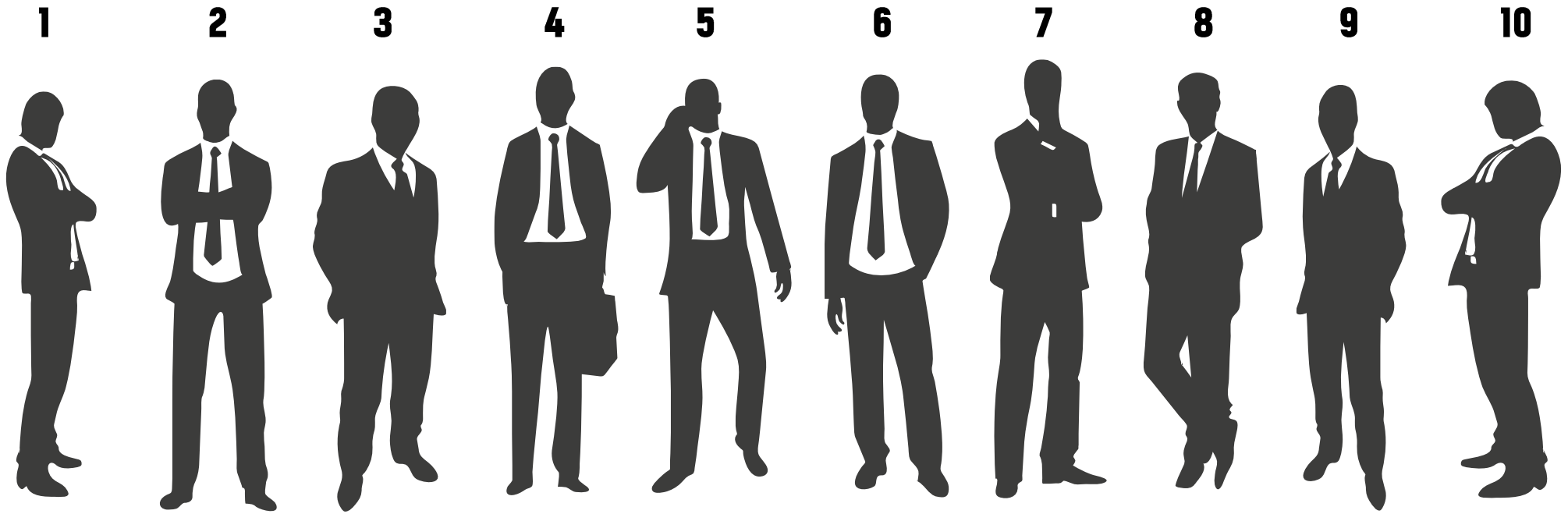
모여 있는 것 흩뜨리고 (기록 관리), 감추던 것(장부 내용)을 드러내자!

A,B,C,D,E 각자의 기록을 중앙기관에서만 관리

A,B,C,D,E 모두 같은 기록을 공유

블록체인의 작동 방식

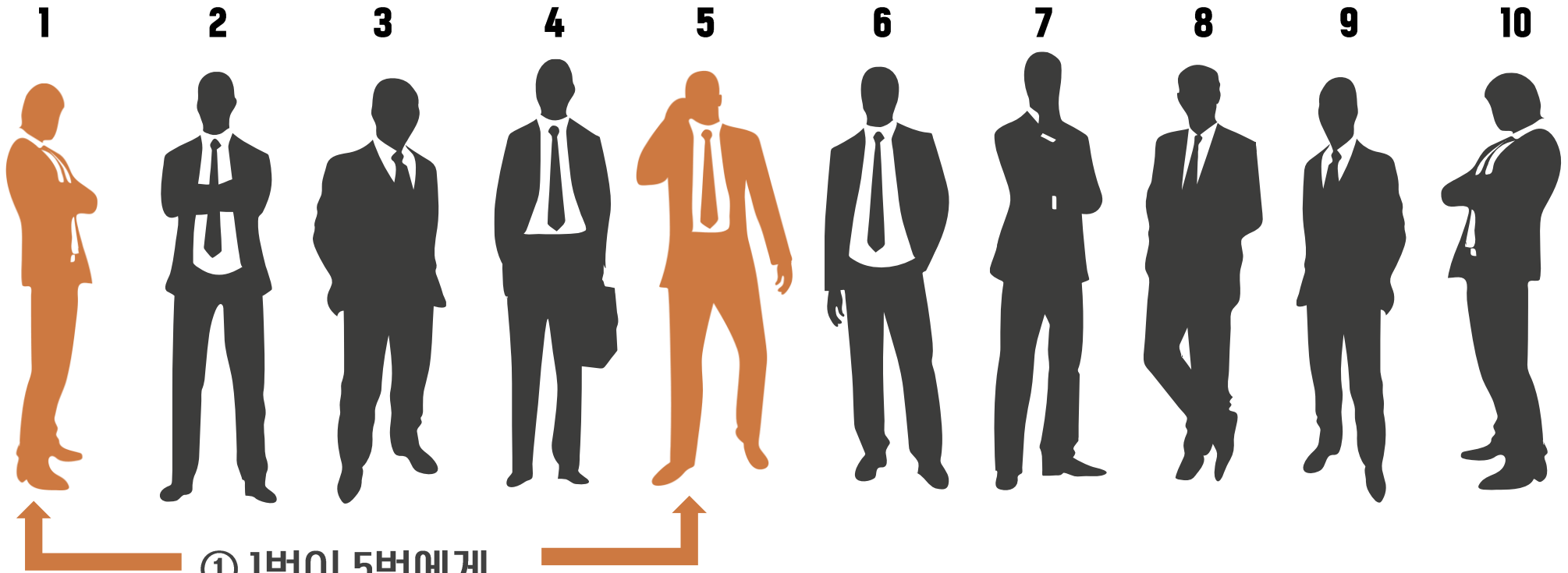
시장참여자 모두가 은행이 되자!



블록체인 생태계 1~10번의 모든 참여자에게는 거래의 모든 내용이 기록된 동일한 장부가 각자에게 주어진다.

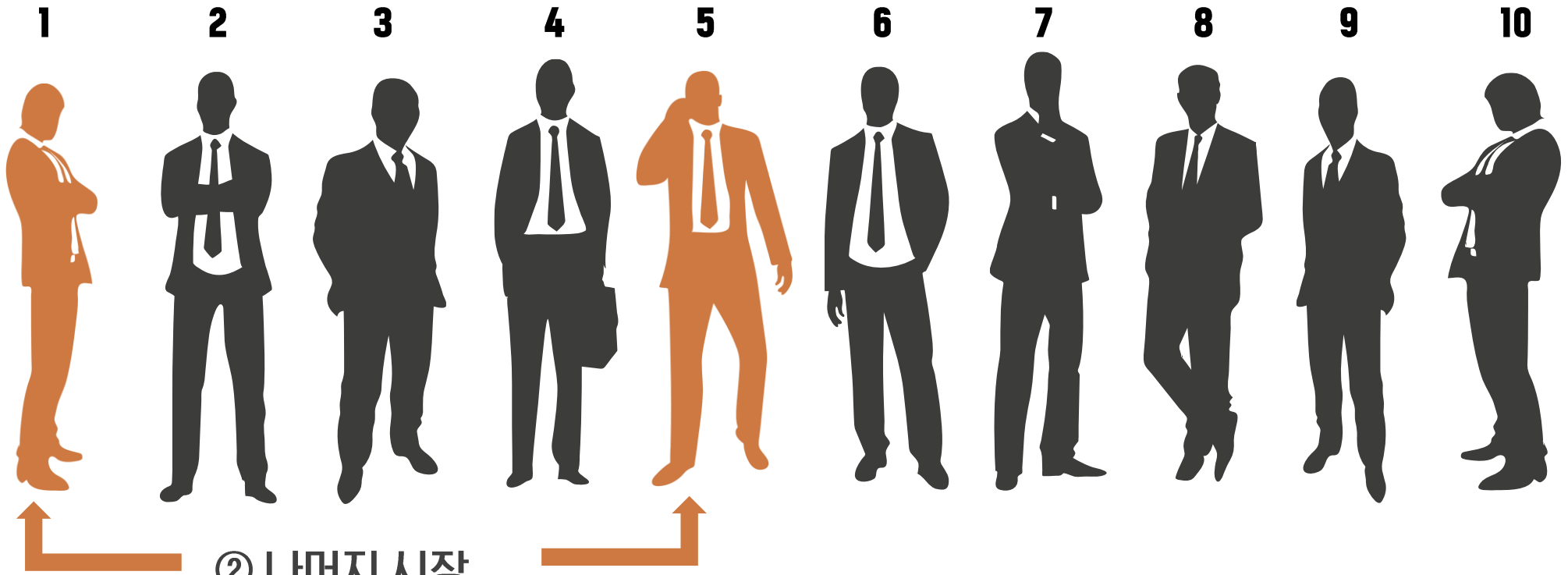
블록체인의 작동 방식

그들 중 누군가가 거래를 원하면!



블록체인의 작동 방식

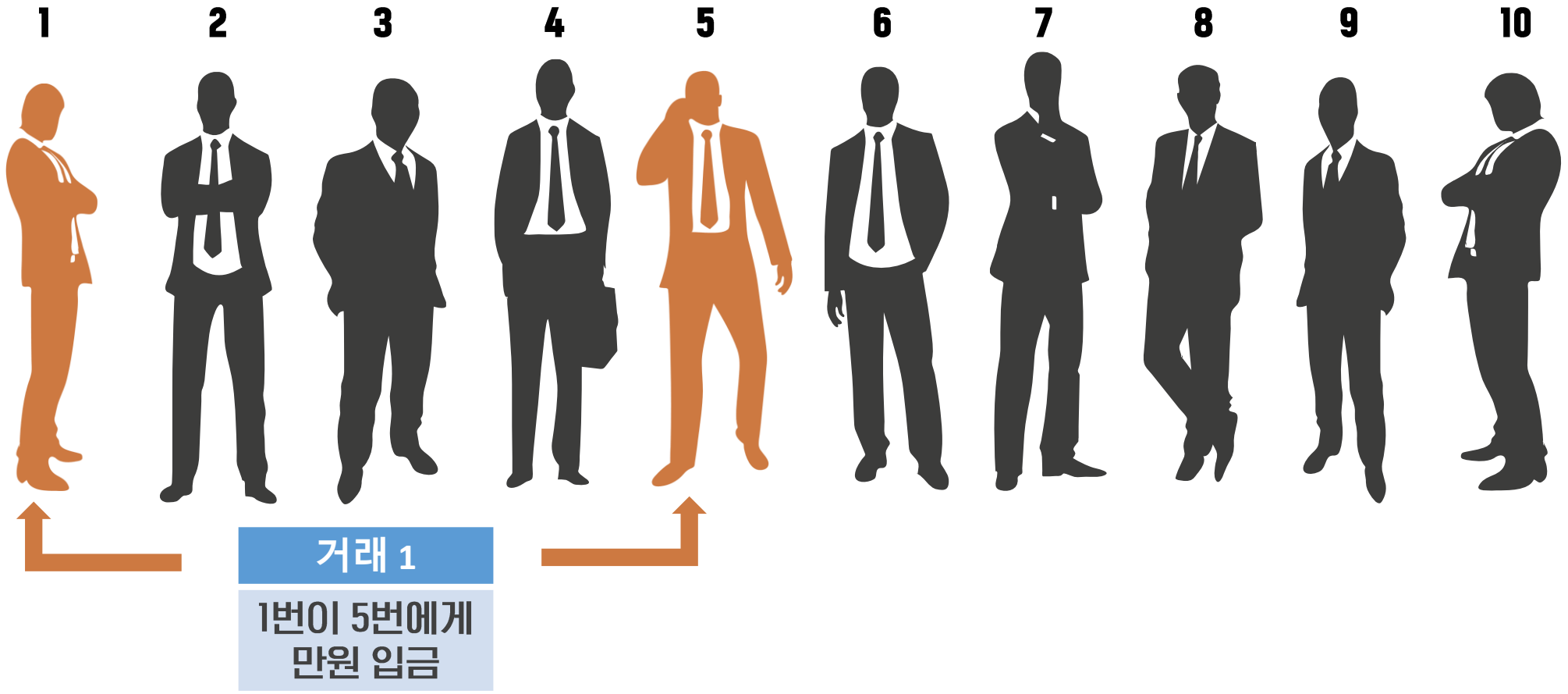
그들 중 누군가가 거래를 원하면!



② 나머지 시장
참여자가 1번에게 잔고가 있는지 확인하고,
거래를 승인 후 송금내역을 기록한다. (은행의 역할)

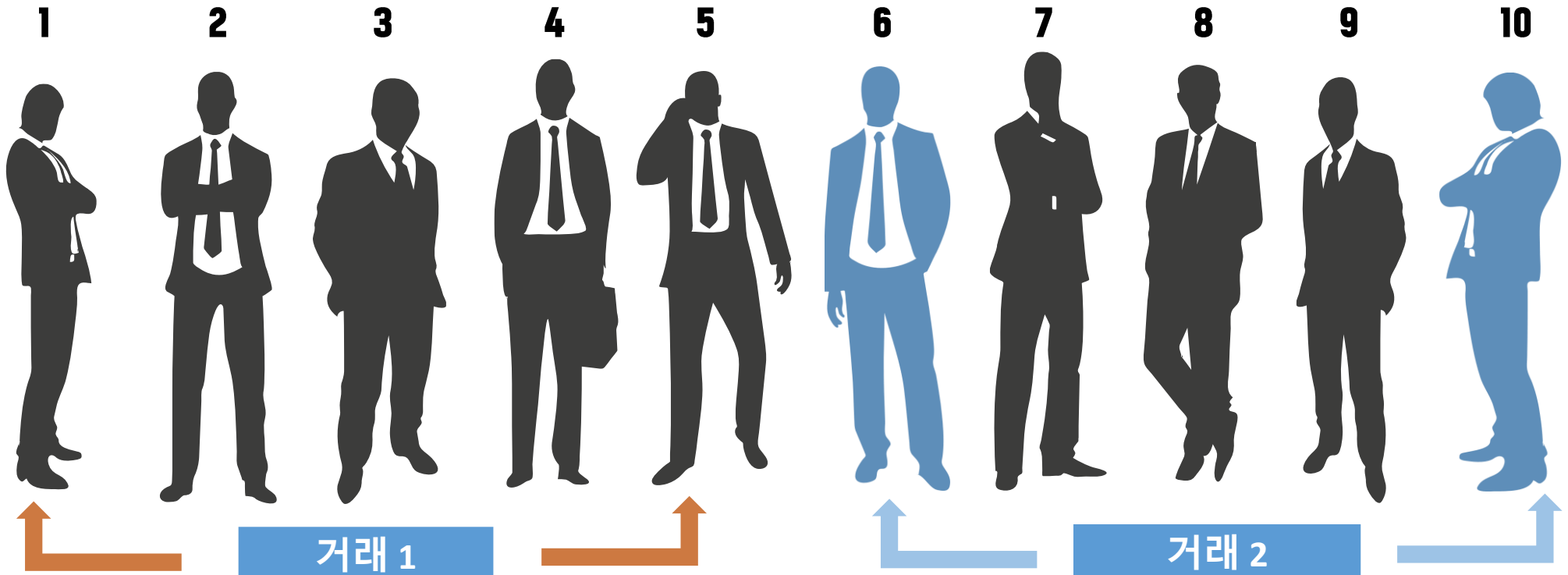
왜 블록체인이라 부르는가?

1과 5의 거래에서 생성한 장부의 기록은 블록(Block)!



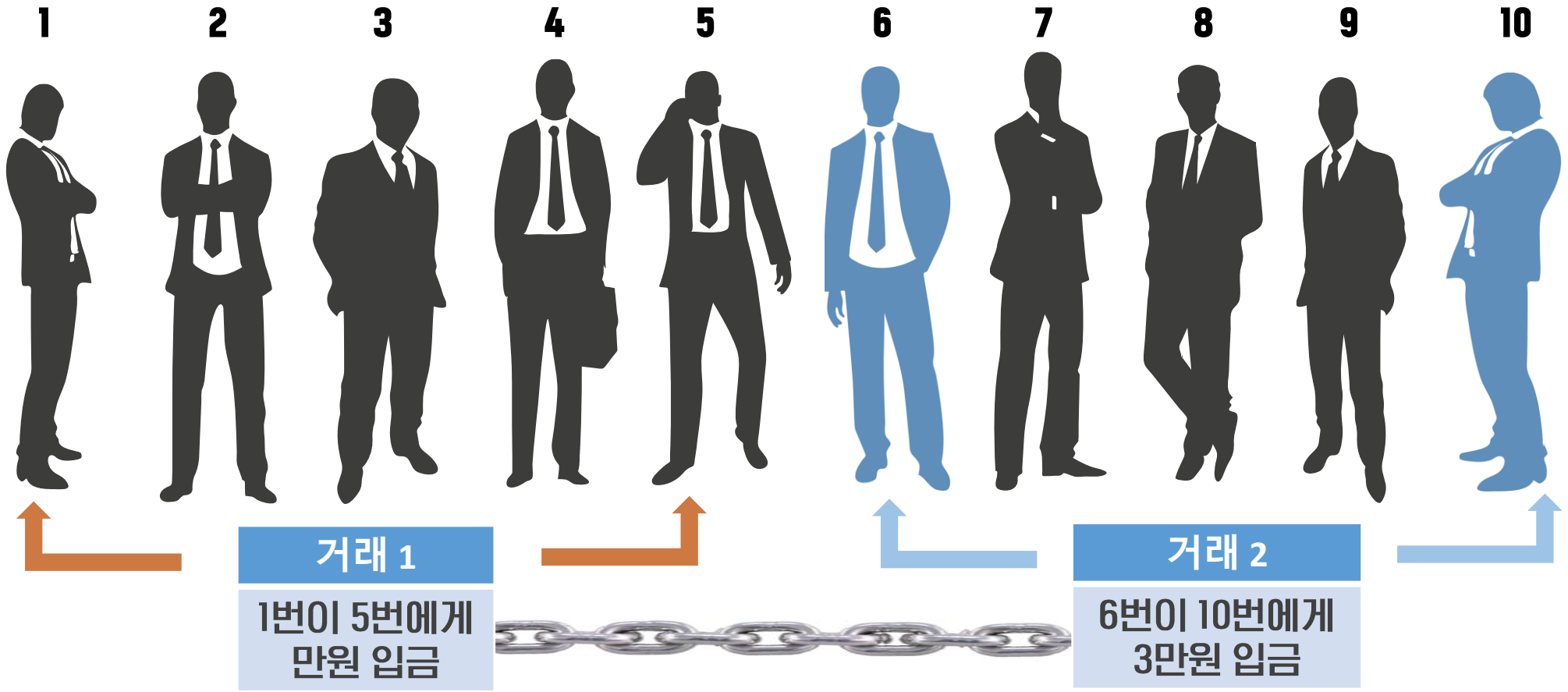
왜 블록체인이라 부르는가?

이후 다른 거래가 발생하면 또다른 블록을 생성 (시간 순)



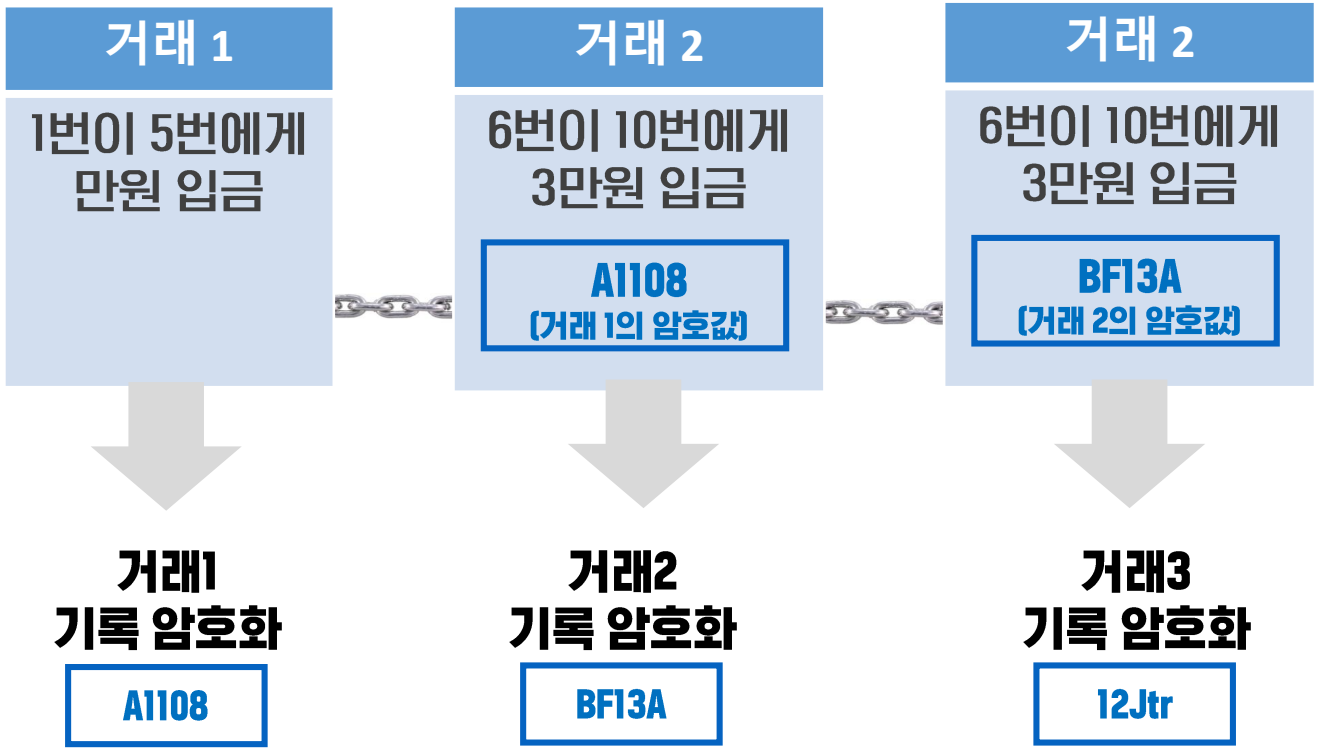
왜 블록체인이라 부르는가?

블록과 블록을 체인(Chain)처럼 단단하게 연결!



어떻게 단단한 체인처럼 연결하는가?

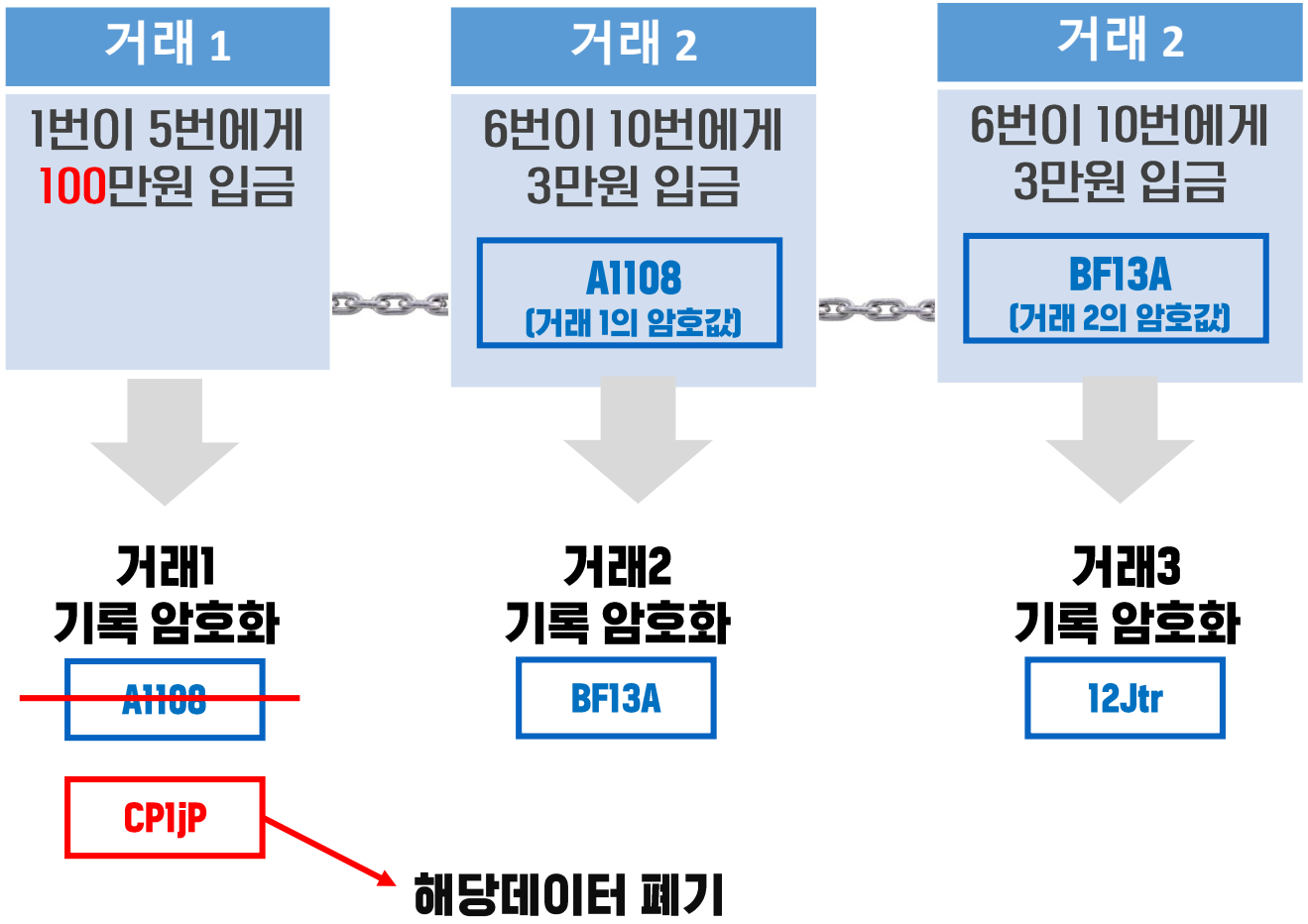
이전의 블록(거래 내역)의 내용을 암호화하여, 다음 거래에 심어 놓는다.



* 참고. 블록의 기록을 암호화 하는 것은 가능하나, 암호화 된 값을 블록의 내용으로 변환하는 것은 불가능 함.

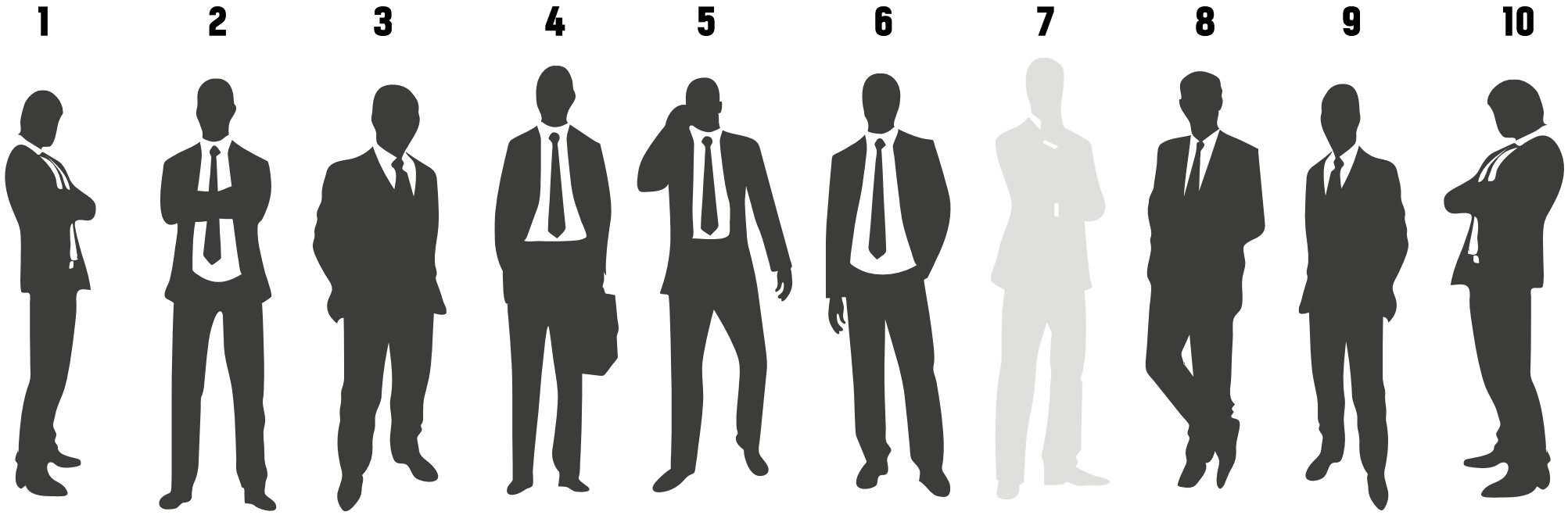
해커가 거래의 기록을 조작한다면?

거래 내역을 변경하면 암호화된 값도 달라지고, 해당 블록은 자동 폐기됨.



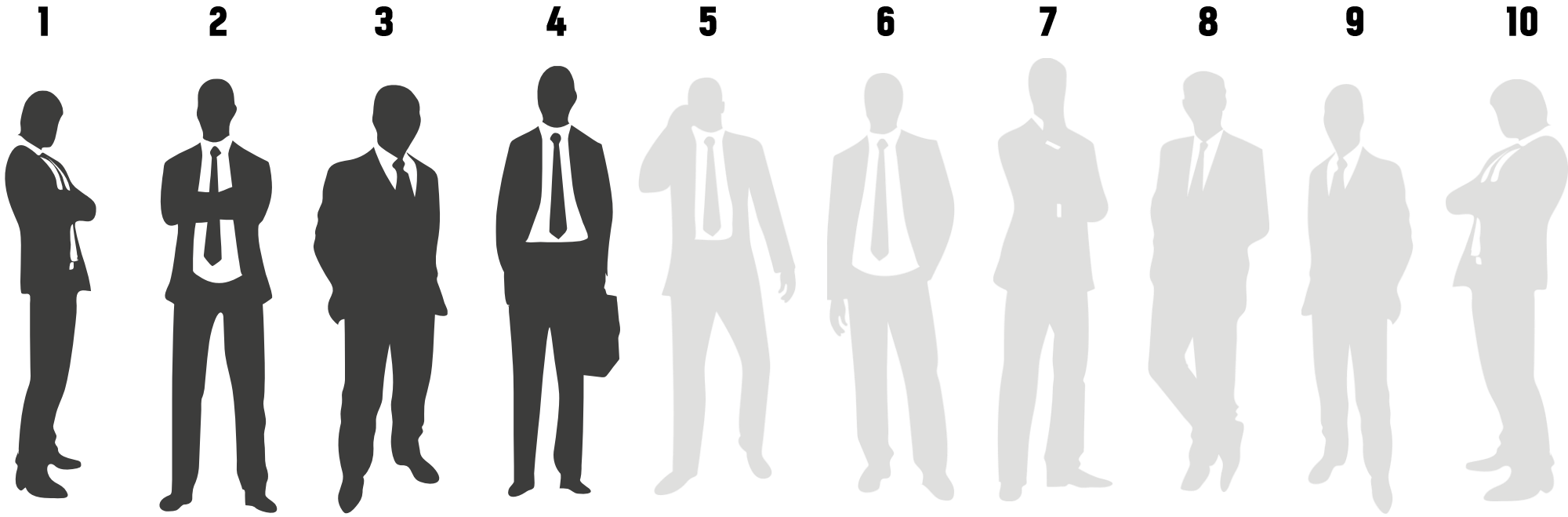
왜 폐기되죠?

블록체인은 생태계에 참여한 모든 사람이 장부를 갖고 있기 때문에,
소수의 잘못된 정보를 폐기함으로 해킹 등의 정보왜곡을 막을 수 있다.



1명이 아니라, 과반이상의 사람이 정보를 왜곡하면?

- 51% 어택 : 네트워크의 참여자의 과반이 조작된 정보를 갖게 되어 가짜 정보가 진짜 정보를 대체하는 위험



10명이니 쉬워 보이나요?

1000명이라면?

블록체인 생태계에서 데이터의 조작은 사실상 불가능에 가깝다!

10만명이라면?

1000만명이라면?

블록체인 기술의 활용영역

비트코인 등의 가상화폐와 금융 뿐만 아니라 물류·유통, 의료데이터,
정부 행정서비스, IoT 플랫폼까지 그 활용 범위를 넓혀갈 것으로 예상 됨.

국내와 해외의 블록체인 기술 활용분야 차이 (출처 : 한국정보화진흥원)