Blockchain
&
Cryptocurrency
Bitcoin

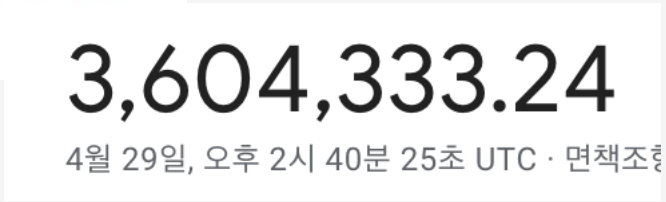
20180488 박준수

Bitcoin: A Peer-to-Peer Electronic Cash System

Smart Contract ?

암호화폐

암호화폐(Cryptocurrency)는 '암호화'라는 뜻을 가진 'crypto-'와 통화, 화폐란 뜻을 가진 'currency'의 합성어로, **분산 장부** (Distributed Ledger)에서 공개키 암호화를 통해 안전하게 전송하고, **해시 함수**를 이용해 쉽게 소유권을 증명해 낼 수 있는 디지털 자산이다



content

1 Blockchain › 2 Hash › 3 PoW
(Proof of Work)

›› 내 코인 만들기... with typescript

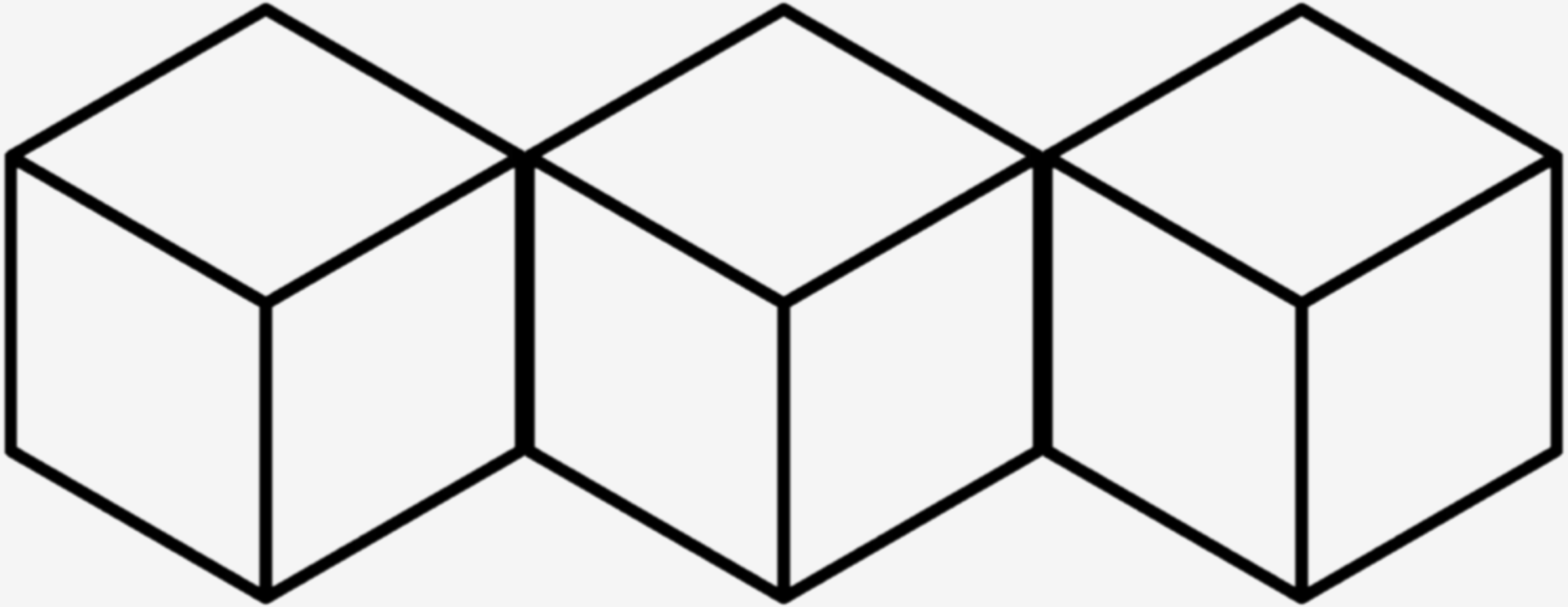
Block

Bitcoin의


```
blocks: [
    {
        hash: "00000000000000000039804e7d4bfe1348746c9abaab42f6dddf71bb0053de",
        ver: 536928260,
        prev_block: "000000000000000003a8ef24695aa3e174ca086930afabe6e3f2eb5f42a87b",
        mrkl_root: "9044311d49a5a9d79be79c67d4a385203a64ca834e045411a7949146732b995b",
        time: 1651462202,
        bits: 386495093,
        next_block: [ ],
        fee: 496973,
        nonce: 450669042,
        n_tx: 172,
        size: 171382,
        block_index: 734511,
        main_chain: true,
        height: 734511,
        weight: 394507,
        tx: [
            {
                hash: "1daba52aa4786594d8518004bf0837779325bdf3621c6e380d57ca941e204d4e",
                ver: 1,
                vin_sz: 1,
                vout_sz: 3,
                size: 296
```

Blockchain

Block들이 연결되어 있는 것 … 특별한 Database



Append Only

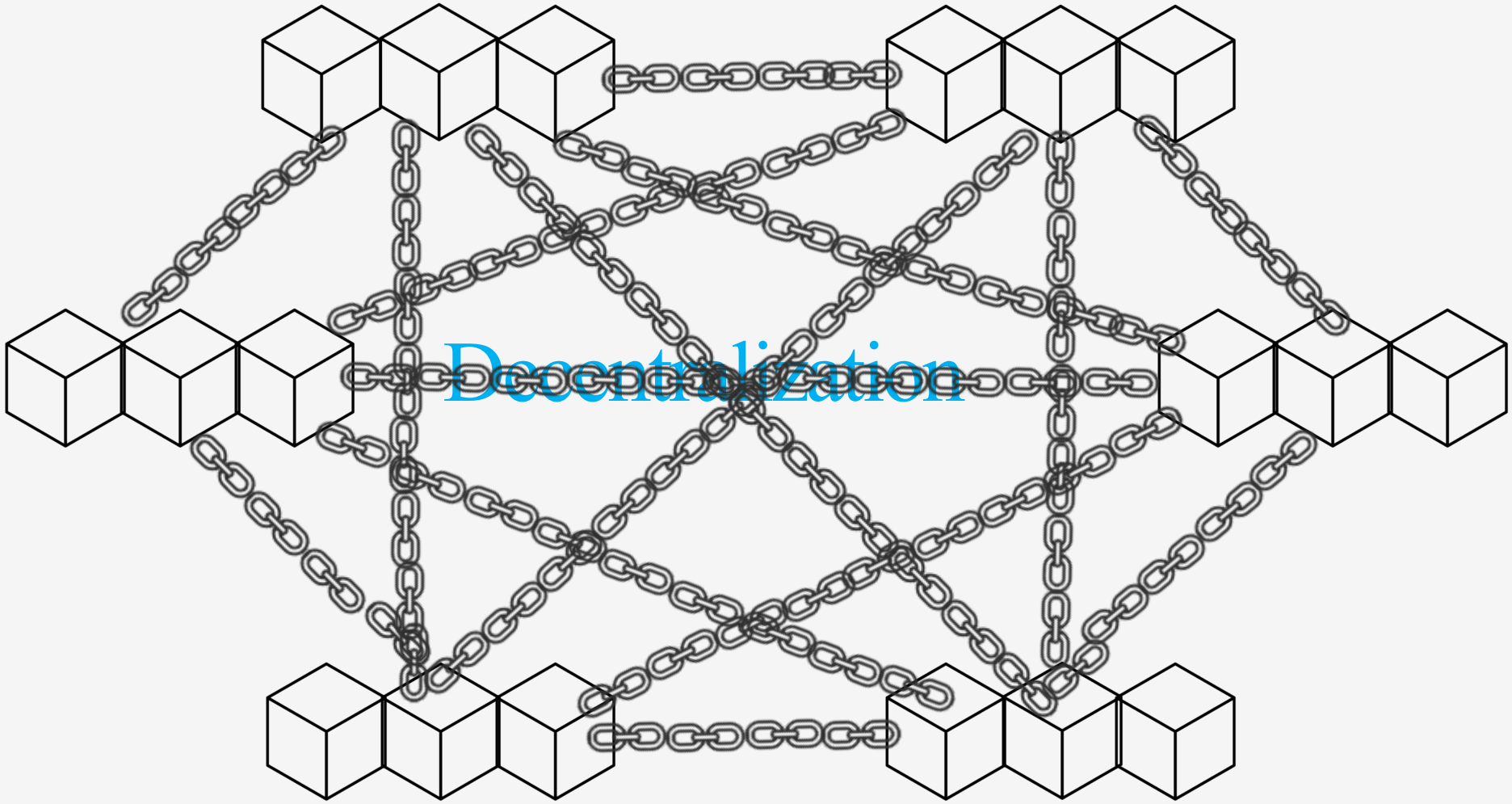
Blockchain


은행이 모든 장부를 관리하는 통일된 거래 내역


'614억 횡령 혐의' 우리은행 직원 동생 영장심사..."돈 출처 몰랐다"
입력 2022.05.01. 오후 2:53 • 수정 2022.05.01. 오후 2:55
추천
댓글
가가
우리은행 직원인 친형과 공모해 우리은행 회삿돈 614억 원을 빼돌린 혐의를 받는 전 모 씨에 대한 구속영장 심사가 진행 중입니다.

Blockchain

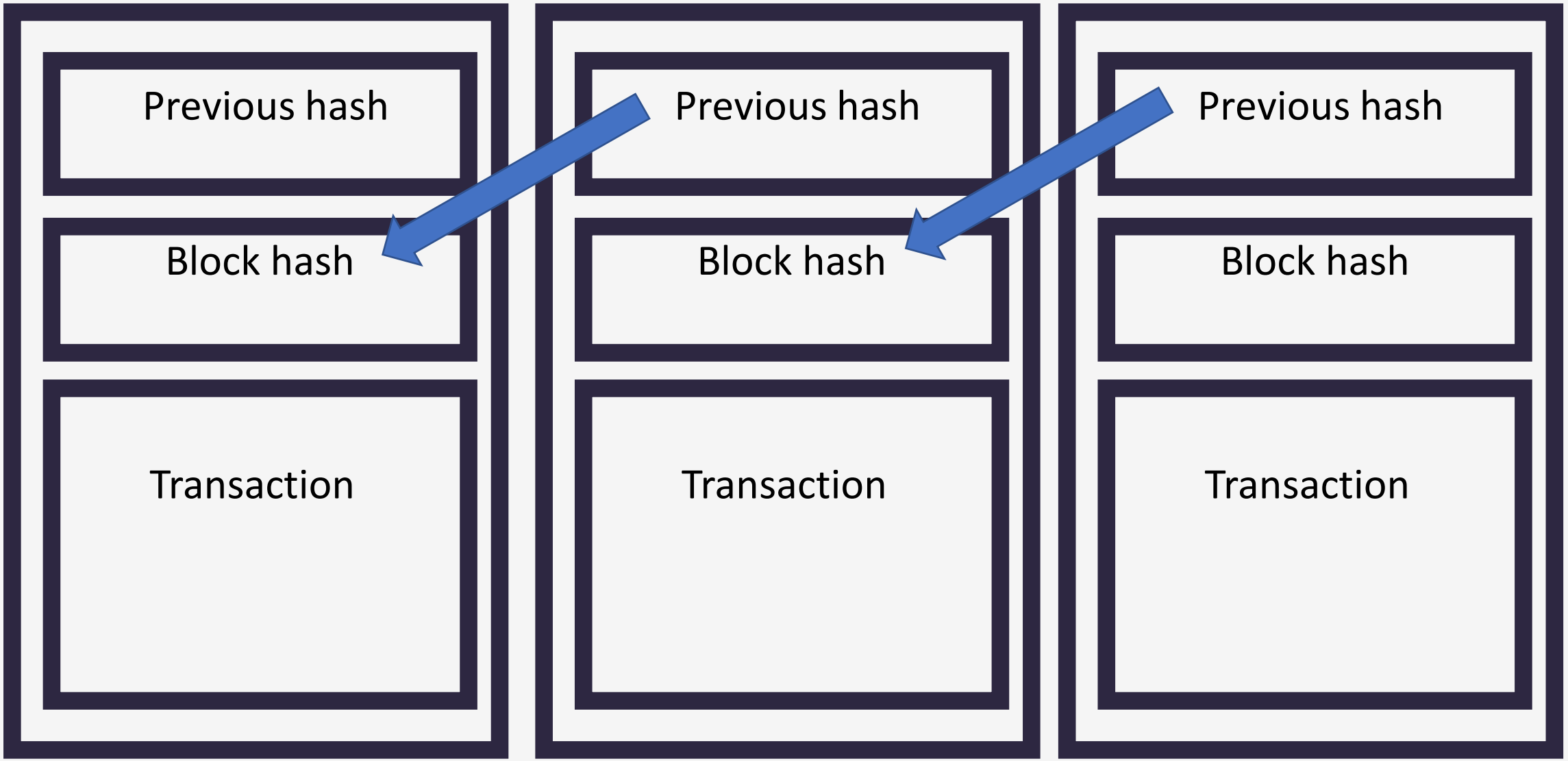
참여한 모든 Node들이 blockchain을 공유, 보관, 관리



Node : P2P 네트워크의 일원으로서 blockchain의 기록을 가지고 있는 사람

Hash

Linked list 형태



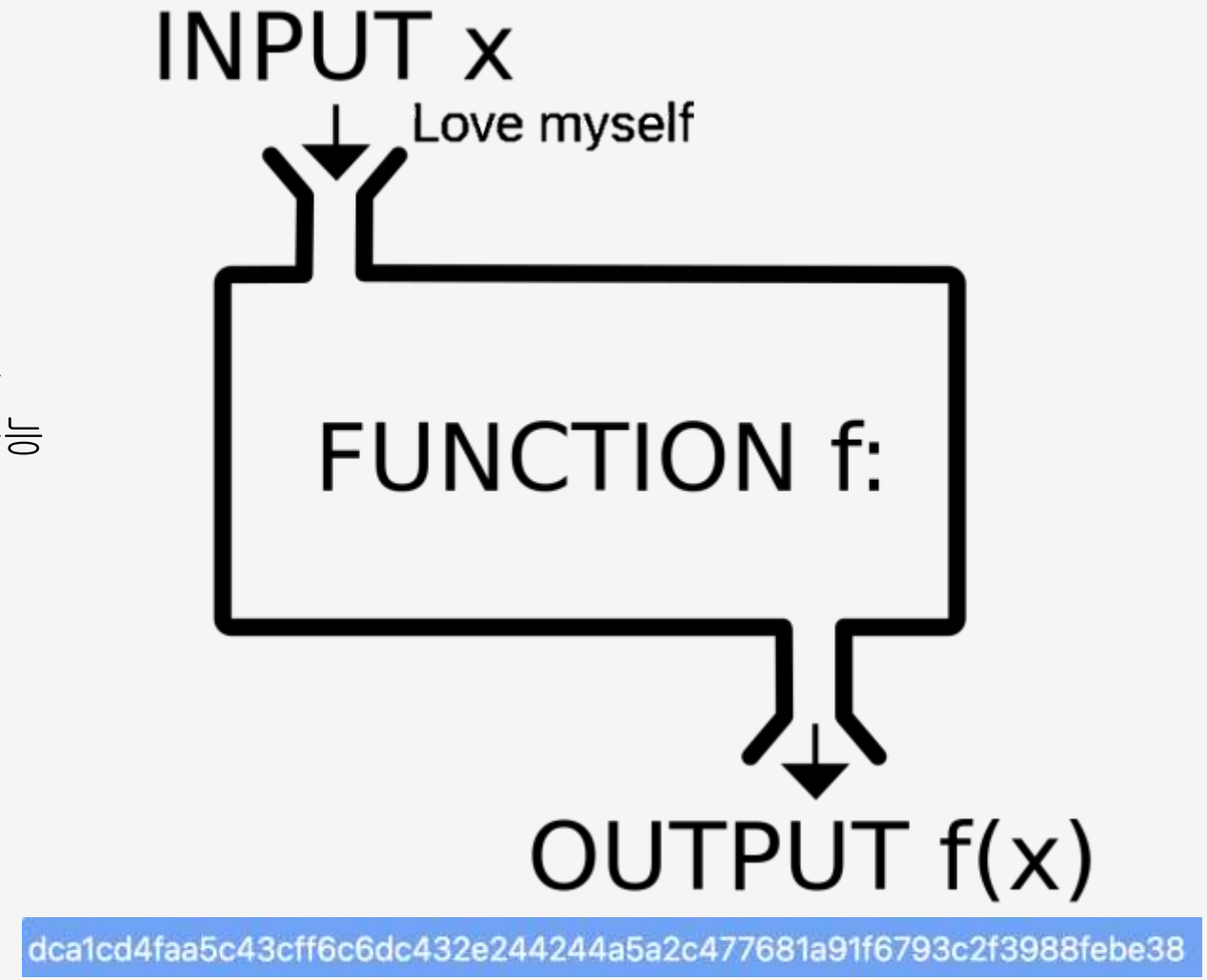
Hash

One way function

x값을 넣으면 금방 y를 구할 수 있으나
y를 가지고 x를 구하는 것은 거의 불가능

Deterministic

어느 input x 의 값을 넣으면 output f(x)의
값은 항상 같은 것으로 정해져 있음



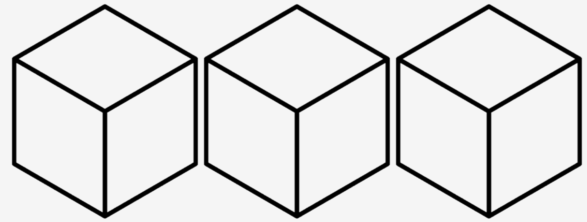
어떻게 블록을 블록체인에 연결하는가?

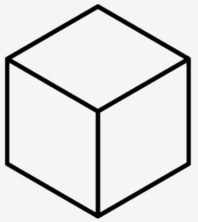
Mining

정상적인 tx이 들어있는 Block을 생성하여 Blockchain으로 연결하는 행위

Mempool

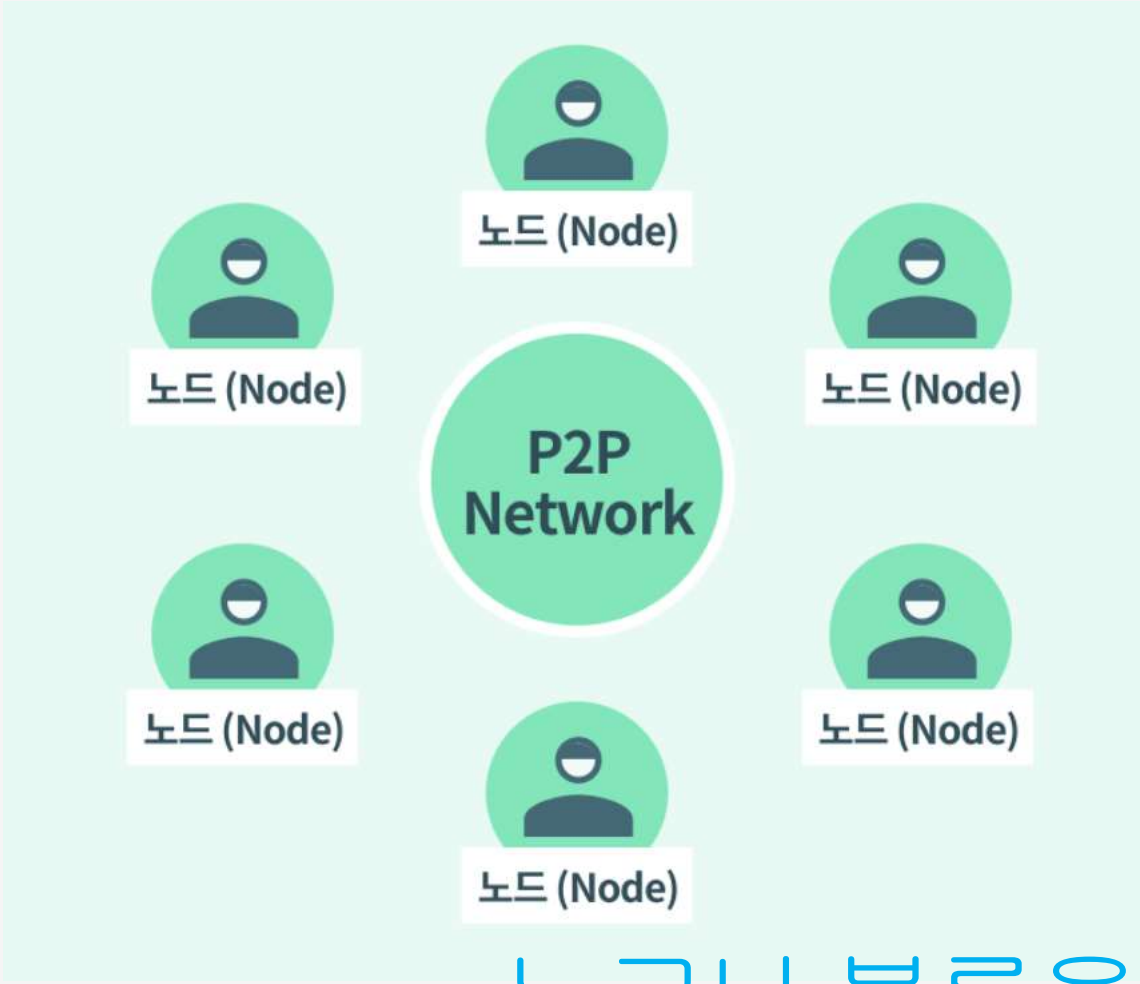
Unverified Txs





Mining

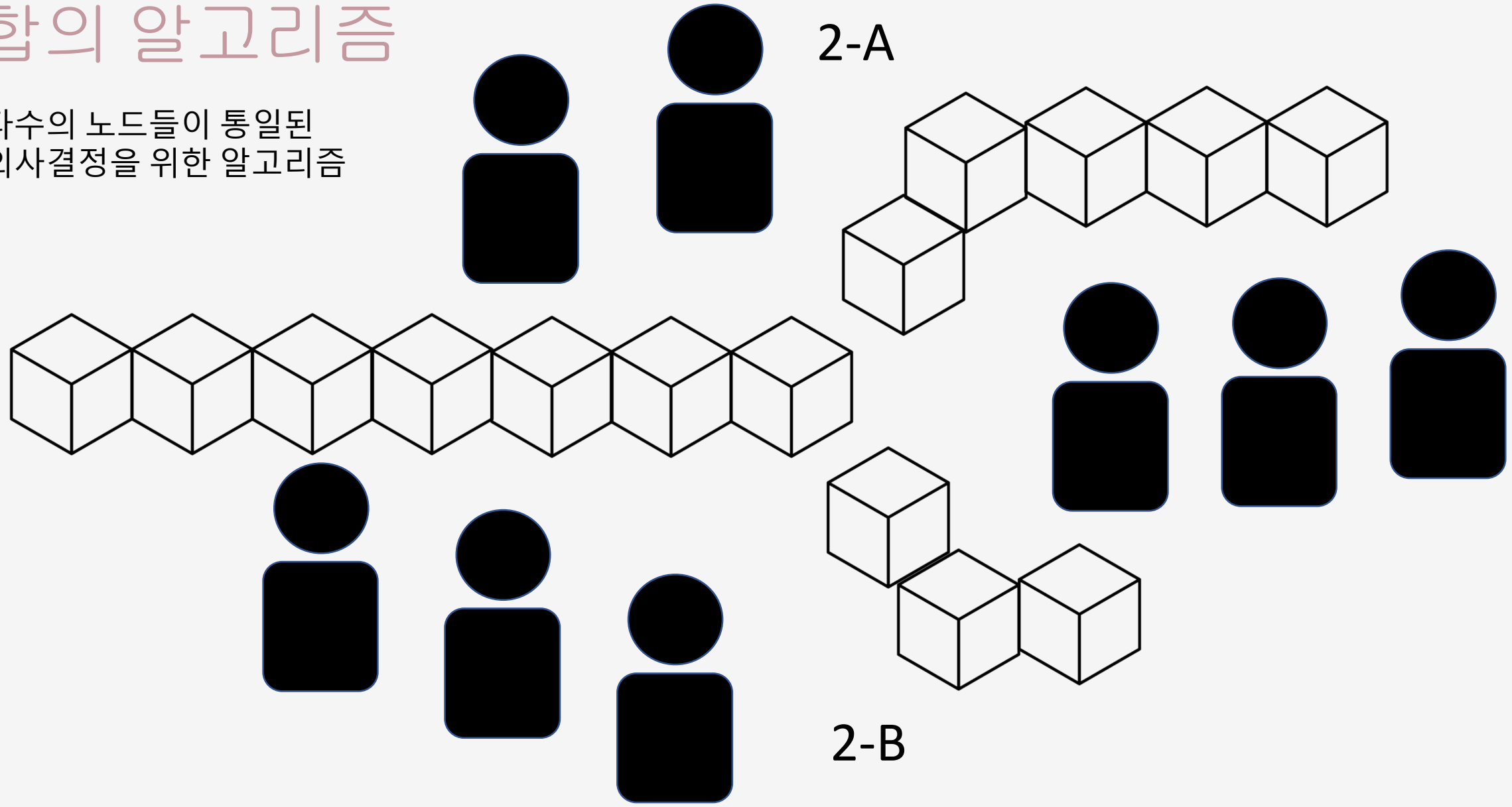
누구든지 거래내역을 검증할 수 있음



누구나 블록을 연결 가능할까?

합의 알고리즘

다수의 노드들이 통일된
의사결정을 위한 알고리즘



Proof of work

풀기 어려운 문제를 빨리 해결한 사람에게 블록을 생성할 수 있는 권한

해시 함수의 결과값이 특정 값보다 작아지도록 하는 입력 값(Nonce)을 찾아라

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

가짜 블록체인이 만들어지는 것을 방지

Miner들은 data를 수정 할 수 없음

Nonce 값만 조절 가능

PoW

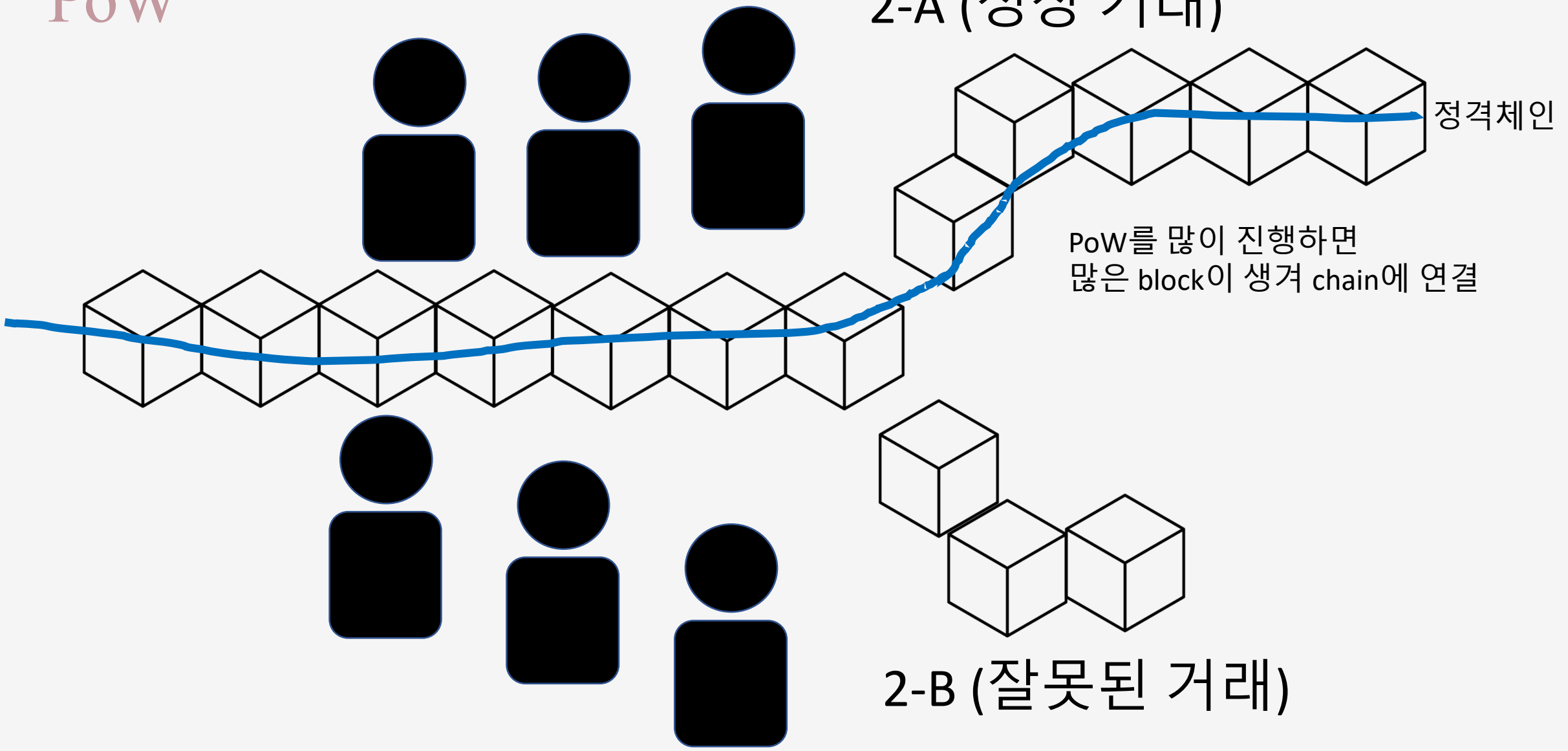
Nonce를 변화시켜 연산을 굉장히 빠르게 수행함

1 **MSI 지포스 RTX 3090 Ti 슈프림 X D6X 24GB 트라이프로져2S**

RTX 3090 Ti / 8nm / 부스트클럭: 1950MHz / 스트림 프로세서: 10752개 / PCIe4.0x16 / GDDR6X(DDR6X) / 출력단자: HDMI2.1, DP1.4 / 부가기능: 제로팬(0-dB기술), 멀티 VGA, 8K 해상도 지원, 4K 해상도 지원, HDR 지원, Dual BIOS, HDCP 2.3 / 사용전력: 최대 480W / 정격파워 850W 이상 / 전원 포트: 16(12+4)핀 x1개 / 3개 팬 / 가로(길이): 338mm / 백플레이트 / LED 라이트 / MYSTIC LIGHT / 그래픽카드 지지대 포함

2,965,980원

PoW



Mining simulation

https://mining-simulator.netlify.app/

지금 비트코인은...?

내 코인 시스템 만들어 보기...

블록 구조

```
let defaultDifficulty: number;
defaultDifficulty = 3;

interface BlockShape {
    height: number;
    prevHash: string;
    hash: string;
    data: string;
    difficulty: number;
    nonce: number;
}
```

블록

```
class Block implements BlockShape {
  public hash: string;
  constructor(
    public height: number,
    public prevHash: string,
    public data: string,
    public nonce: number,
    public difficulty: number
  ) {
    this.hash = Block.calculateHash(prevHash, height, data, nonce, difficulty);
    this.difficulty = 3;
  }
  public mine() {…
  }
  static calculateHash(…
  }
}
```

```
static calculateHash(
  prevHash: string,
  height: number,
  data: string,
  difficulty: number,
  nonce: number
) {
  const toHash = `${prevHash}${height}${data}${difficulty}${nonce}`;
  return crypto.createHash("sha256").update(toHash).digest("hex");
}
```

sha256을 사용하여 Hashing

Default = 3

```
class Blockchain {
  private blocks: Block[];
  constructor() {
    this.blocks = [];
  }
  private getPrevHash() {…
  }
  private getDiff() {…
  }
  public addBlock(data: string) {…
  }
  public getBlocks() {
    return [...this.blocks];
  }
}
```

```
private getPrevHash() {
  if (this.blocks.length === 0) return "";
  else return this.blocks[this.blocks.length - 1].hash;
}
private getDiff() {
  if (this.blocks.length === 0) return defaultDifficulty;
  else return this.blocks[this.blocks.length - 1].difficulty;
}
```

getPrevHash(): 이전 hash값

getDiff() : difficulty를 가져옴
(난이도 조정기능 필요...)

블록 mining

```
public mine() {
  let target: string = "0".repeat(this.difficulty);
  let hashing: string = this.hash;
  while (true) {
    if (hashing.startsWith(target)) {
      this.hash = hashing;
      break;
    } else {
      this.nonce++;
      hashing = Block.calculateHash( …
      );
    }
  }
}
```

블록체인 결과

```
[nodemon] starting `ts-node src/index.ts`
[
  Block {
    height: 1,
    prevHash: '',
    data: 'Genesis',
    nonce: 2969,
    difficulty: 3,
    hash: '000bec1b05bb4001d57e365c935672b75d5429ef09e99b5f4ed1657d63e1b715'
  },
  Block {
    height: 2,
    prevHash: '000bec1b05bb4001d57e365c935672b75d5429ef09e99b5f4ed1657d63e1b715',
    data: 'Second',
    nonce: 1426,
    difficulty: 3,
    hash: '000e4196179e2359b184346ec4856ea8d90f61fb288e3ab3346135cbe391d7e3'
  }
]
```

격하게

감사합니다

References

Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008

https://ko.wikipedia.org/wiki/%EC%95%94%ED%98%B8%ED%9%94%ED%8F%90

https://www.banksalad.com/contents/%EC%89%BD%EA%B2%8C-%EC%84%A4%EB%AA%85%ED%95%98%EB%8A%94-%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8-%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8%EC%9D%98-%EC%9B%90%EB%A6%AC-%EC%B1%84%EA%B5%B4-%ED%95%B4%EC%8B%9C-%EA%B7%B8%EB%A6%AC%EA%B3%A0-%EC%9E%91%EC%97%85%EC%A6%9D%EB%AA%85-qvCud

https://tenor.com/view/mine_doge-gif-24806628