GIST

Goal of this lecture note

- Need for Proof-of-Work (PoW)
- PoW Puzzles
- Difficulty Level of Puzzles
- Probability of Mining Success
- AI-IM-To-Po Theory

1 Need for Proof-of-Work (PoW)

- Blockchain
  is a ledger and a technology.
  - A digital file it is.
  - Content can be copied and altered easily.
  - A novel way is to resolve the problem of forgery and unwanted alterations:
    - Each block is summarized.
    - This summary shall be good enough.
    - Only the block with the proof of work included can be connected to the existing chain of blocks.

GIST

1 Need for Proof-of-Work (PoW)

- Blockchain
  - Revolutionary new idea!
    - Any single computer cannot find a good block summary within a given amount of computing time.
    - If the number of computers is large enough and all are simultaneously working on finding good summary of a block, one computer among them can come out successful within the desired time.

1 Need for Proof-of-Work (PoW)

- Blockchain
  - Revolutionary new idea!
    - A reward is given to this computer which has found a good block summary.
    - Once completed, a new race is set and started again for a new block formation.
    - The more computers are gathered and participate in the race, the safer the system becomes.

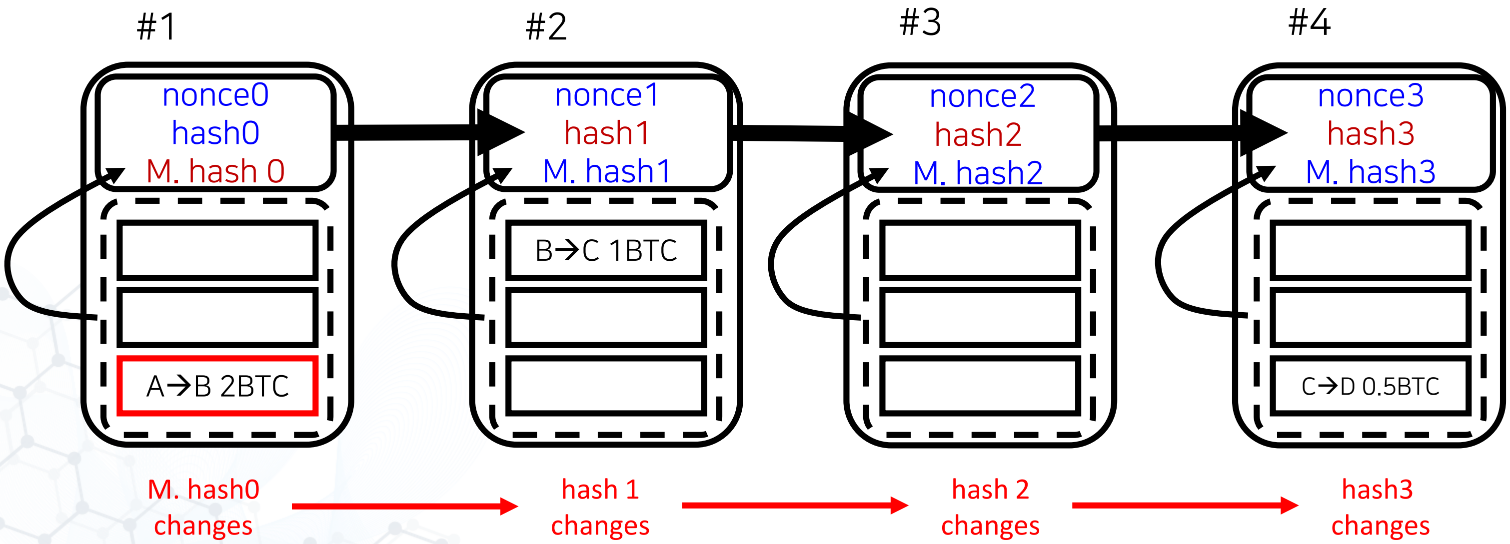
GIST

1 Need for Proof-of-Work (PoW)

- Content in the blockchain cannot be changed.
  - What happens when any alteration is made?
  - Any small alteration is easily noticeable!
  - An unnoticeable change is possible, but it requires a complete alteration.
  - The complete job is to redo all the hashes of the following blocks.
  - PoW is imposed in each block and thus the whole job cannot be made easily.

1 Need for Proof-of-Work (PoW)

- Content in the blockchain cannot be changed, why?



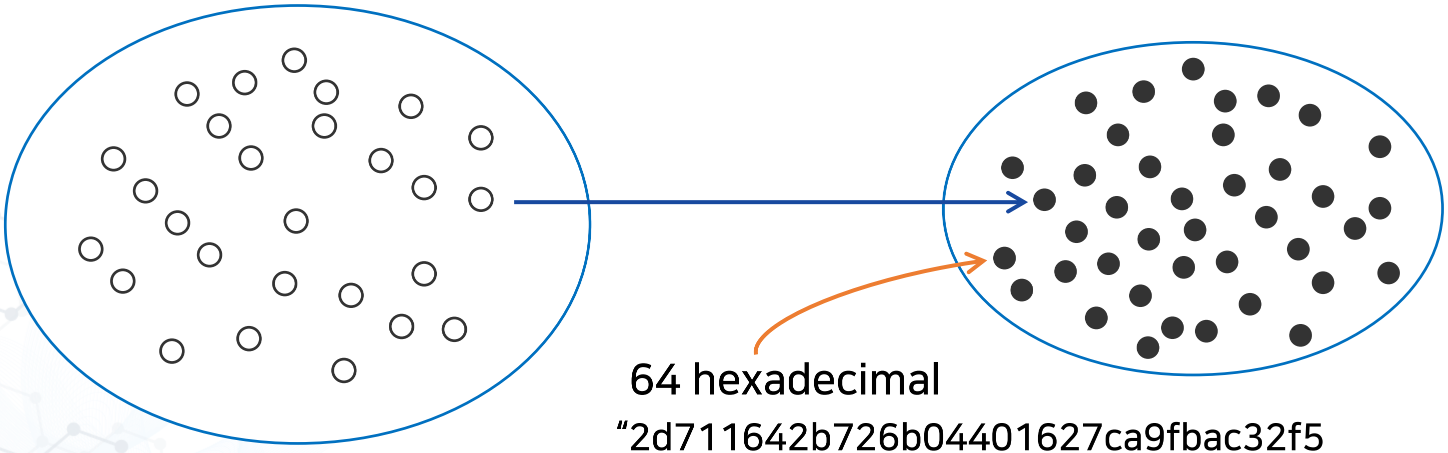
2 PoW Puzzles

- Making PoW puzzles
  - Bitcoin uses SHA256
  - Recall SHA is *oneway* and *collision free*.

2 PoW Puzzles

- SHA256, $F(x) = y$

$X = \{x | x \text{ is a message up to 1 Mbyte in size}\}$ $\quad$ $Y = \{y | y \text{ is a 256bit string}\}$



"2d711642b726b04401627ca9fbac32f5
c8530fb1903cc4db02258717921a4881"

GIST

2 PoW Puzzles

- Finding Good Block Summary
  - Function F takes x and gives output y

$$y = F(x)$$

  - x is block header (BH), i.e., F(BH) = hash.
  - Then, it can be written as

F(B.H.: nonce) < Target   PoW Ineq.

  - For a block, find a nonce that satisfies the above inequality (Work)
  - Record the nonce in the block header. (Proof)

GIST

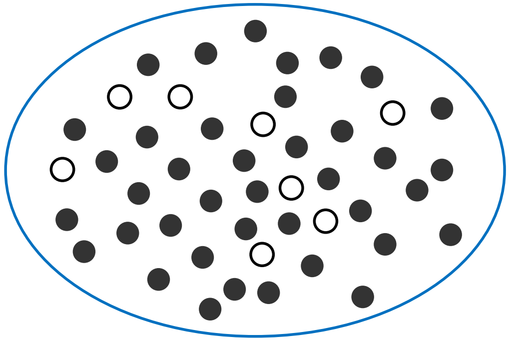
2 PoW Puzzles

- Toy puzzle
  - White and black balls.
  - There are 2^6 black balls.
  - Balls are numbered, i.e., hashes.
  - Let Target be 2^3=8.
  - Pick a nonce and run SHA-256.

Total no. of balls $2^6 = 64$
Target = 2^3 0 0 1 0 0 0
A = {Balls < Target}
$2^3 - 1 = 7$ 0 0 0 1 1 1
6 0 0 0 1 1 0
5 0 0 0 1 0 1
...

What is the probability that a while ball is picked?

$$p = 2^3/2^6 = 1/8$$



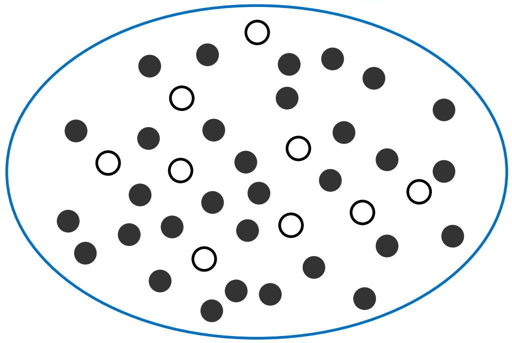
2 PoW Puzzles

- Bitcoin puzzle
  - Hashes are strings of 256 bits.
  - There are 2^{256} hashes in Y.
  - Let Target be $2^{256-16}=2^{240}$.

What is the probability that the hash satisfies the PoW?

$$p = 2^{240}/2^{256}$$
$$= 2^{-16}$$
$$= 1/64000$$

$Y = \{y | y \text{ is a 256bit string}\}$



White balls are
64 hexadecimals with 4 leading zeros

"00001642b726b04401627ca9fbac32f5
c8530fb1903cc4db02258717921a4881"

GIST

3 Difficulty Level of Puzzles

- The probability p that a CPU solves (PoW) in a single cycle, given the first four strings are zeros?
  - Any hash value looks line this:
    "2d711642b726b04401627ca9fbac32f5c
    8530fb1903cc4Db02258717921a4881"
  - A good hash value looks like this:
    "0000f727854b50bb95c054b39c1fe5c92
    e5ebcfa4bcb5dc279f56aa96a365e5a"
    - c = the size of Y the set of all hash values = 2^{256}
    - a = the size of A the set of wanted hash values $= 2^{(256-16)} = 2^{240}$
    - p = a/c = $2^{-16} = 1/2^{16} \sim 1/64000$

3 Difficulty Level of Puzzles

- Proof of Work is a ALone IMpossible Together Possible (Al-IM-To-Po) Problem!
  - Let there be a CPU which can take one input and gives one output.
  - What is the probability that this CPU finds a good summary in a single hash cycle?

$$p = a/c = 2^{-16} = 1/64000$$

  - Difficulty of the PoW puzzle can be adjusted by varying the size of a.
  - Thus, p represents a difficulty of the puzzle.

GIST

4 Probability of Mining Success

- Given the difficulty p, we aim to find Probability of Mining Success.

GIST

4 Probability of Mining Success

- Definition: Success Random Variable K.
  Let $K = 1, 2, 3, \cdots$, denote the index of the hash at which PoW success occurs.
  - For example, $K = 4$ means that PoW success comes exactly at the 4th hash.
  - This is a random variable since the draw of a successful hash value is a random experiment.

GIST

4 Probability of Mining Success

- Definition: Hash Rate of CPU.
  - The hash rate of a CPU is defined as number hashes in a unit time.
  - For example, the hash rate of a CPU which can do 100 hash cycles in 1 second is 100 hashes/sec.

4 Probability of Mining Success

- ASIC Mining Hardware

Bitcoin Mining Hardware Comparison

Pic	Miner	Hash Power	Price	Buy
	Antminer S9	14.0 TH/s	$3,000	
	Antminer R4	8.6 TH/s	$1,000	

출처: https://www.buybitcoinworldwide.com/mining/hardware/

GIST

4 Probability of Mining Success

- Definition: Success Random Variable K.
  Let K = 1, 2, 3,⋯, denote the index of the hash values at which the PoW success occurs
  - What is the probability that this CPU with rate 100 hashes/sec solves PoW in 1 second? Use $p = 10^{-6}$.

$$P_p\{K \le k\} =: P_{Geom}(p, k = 100)$$

$$= p + (1-p)p + \cdots + (1-p)^{k-1} p$$

$$\sim 100 * p$$

$$= 10^{-4} \quad (2.384\text{e-}5 \text{ exact})$$

GIST

4 Probability of Mining Success

- (PMF) What is the probability that a CPU solves PoW exactly at the k-th hash?

$$P_{pmf}(p,\ k) := P_p\{K \le k\} - P_p\{K \le k-1\}$$

$$= P_p\{K = k\}$$

$$= p + (1-p)p + (1-p)^2 p + \cdots + (1-p)^{k-1} p$$

$$-\left(p + (1-p)p + (1-p)^2 p + \cdots + (1-p)^{k-2} p\right)$$

$$= (1-p)^{k-1} p \qquad \text{for any } k = 1, 2, 3, \cdots$$

4 Probability of Mining Success

- Average no. of hashes for a PoW success
  - What is the average number of hashes for a PoW success for a given puzzle difficulty p?

$$
\begin{aligned}
\mathbb{E}\{K\} &= \sum_{k=1}^{\infty} P_{pmf}(p,\ k)\ k \\
&= \sum_{k=1}^{\infty} (1-p)^k\ p\ k \\
&= \frac{1}{p} \\
&= 10^6 \quad \text{[hashes/block]}
\end{aligned}
$$

GIST

4 Probability of Mining Success

- $P_{geom}(p, k)$ is the CDF of PoW success in k (hash) hashes.
- Consider the distribution of no success in k hashes.

$$
\begin{aligned}
P_p\{K > k\} &= 1 - P_p\{K \le k\} \\
&= \sum_{j=1}^{k} (1-p)^{j-1} p \\
&= \sum_{j=k+1}^{\infty} (1-p)^{j-1} p \\
&= (1-p)^k \sum_{j=1}^{\infty} (1-p)^{j-1} p \\
&= (1-p)^k
\end{aligned}
$$

GIST

5 AI-IM-To-Po Theory

- Theorem 1. (Alone) The CDF $P_{geom}(p, k)$, the probability of PoW success in k hashes, can be expressed as

$$
\begin{aligned}
P_p\{K \le k\} &= 1 - P_p\{K > k\} \\
&= 1 - (1-p)^k.
\end{aligned}
$$

GIST

5 AI-IM-To-Po Theory

- Let $P_1\ (p, k)$ be the probability that a CPU solves a PoW with p in k hashes.

- What is the probability that at least one CPU out of N CPUs finds a good block hash?

5 AI-IM-To-Po Theory

- Theorem 2. There are N CPUs working independently on the PoW puzzle with difficulty p. The probability P_2 that at least one CPU out of N finds a good block summary in k hashes is given by

$$
\begin{aligned}
P_2(N, p, k) &= \Pr\{\text{at least one CPU success}\} \\
&= 1 - \Pr\{\text{no CPU success}\} \\
&= 1 - [1 - P_1(p, k)]^N
\end{aligned}
$$

GIST

5 AI-IM-To-Po Theory

- Corollary 3. (All Together) There are $N = k$ CPUs which work independently on the PoW puzzle with difficulty p.
  The probability P_{all} that at least one CPU out of N finds a good block hash in a single hash is given by

$$
\begin{aligned}
P_{\text{all}}(N=k, p) &= \mathrm{P}_2(N, p, k=1) \\
&= 1 - \Pr\{\text{no CPU success}\} \\
&= 1 - [1-p]^N .
\end{aligned}
$$

$$
\begin{aligned}
P_p\{K \le k\} &= 1 - P_p\{K > k\} \\
&= 1 - (1-p)^k .
\end{aligned}
$$

GIST

5 AI-IM-To-Po Theory

- From the Alone theorem and All-together corollary, one can notice that the distributions are the same, given $N = k$.

$$P_{geom}(p, k) = P_{\text{all}}\,(N{=}k, p)$$
$$= 1 - \Pr\{\text{no CPU success}\}$$
$$= 1 - [1 - p]^N$$

GIST

5 AI-IM-To-Po Theory

- Let the difficulty of puzzle be given with $p = 10^{-20}$.
- Assume a mining chip with hash rate $R_{chip} = 10^{12}$ hashes/sec.
- Give answers on the average numbers.

1. How many hashes does it take for this chip to make a success?
2. How long does it take for this chip to make a success?
3. How many chips do you need to make a success in a single unit of time?

5 AI-IM-To-Po Theory

- Let the difficulty of puzzle be given with $p = 10^{-20}$.
- Assume a mining chip with hash rate $R_{chip} = 10^{12}$ hashes/sec.

1. How many cycles does it take for this chip to make a success?

   $\mathrm{E}\{K\} = 10^{20}$ [hashes/block].

GIST

5 AI-IM-To-Po Theory

- Let the difficulty of puzzle be given with $p = 10^{-20}$.
- Assume a mining chip with hash rate $R_{chip} = 10^{12}$ hashes/sec.

2. How long time T_{block} for this chip to make a success?

$$T_{block} = E\{K\} / R_{chip}$$

$$= 10^{20}/10^{12} \text{ [sec/block]}$$

$$= 10^{8} \text{ [sec/block]}$$

$$= 3.15 \text{ [year/block]}$$

GIST

5 AI-IM-To-Po Theory

- Let the difficulty of puzzle be given with $p = 10^{-20}$.
- Assume a mining chip with hash rate $R_{chip} = 10^{12}$ hashes/sec.

3. How many chips do you need to make a success in a second?

$$T_{block} = E\{K\} / (R_{chip} \times N_{chip})$$

$$N_{chip} = E\{K\} / (R_{chip} \times T_{block})$$

$$= 10^{20}/(10^{12} \times 1)$$

$$= 10^{8}$$

$$= 100 \text{ Million}$$

5 AI-IM-To-Po Theory

- From previous examples, we now understand what we mean by the AI-IM-To-Po theory.
- The Alone-theorem shows that it takes about 3.15 years to a single PoW success, if a single chip is used.
- The All-together corollary indicates that it takes 100 Million such chips working together for a single PoW success.