



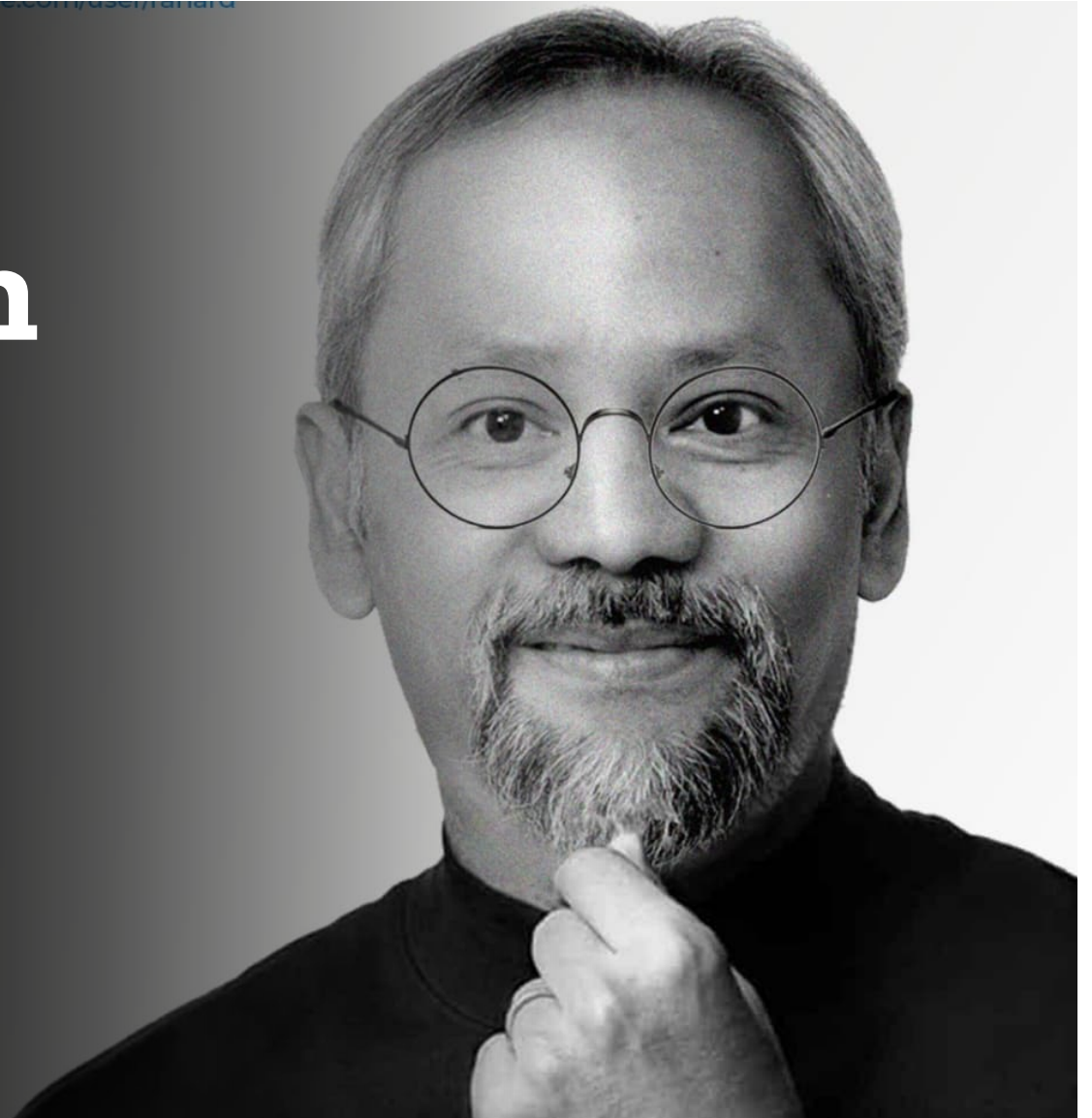
# Introduction to Blockchain

---

Budi Rahardjo

@rahard

2024



Have you heard of **Bitcoin**?  
Cryptocurrency? NFT?



# Ghazali NFT

# Foto Rektor ITB di-NFT-kan

the finery report

Masuk ke ITB, kukira aku akan mendapatkan kesempatan yang berimbang bagi semua. Tanpa melihat seperti apa aku dahulu, tanpa melihat rupa dan dari mana aku berasal, juga tanpa melihat seberapa banyak materi yang kumiliki. Padahal setahu, setiap warga negara memiliki hak yang sama untuk memperoleh pendidikan yang bermutu. Kukira juga, hati seorang ibu memiliki kelulusan yang tak terbatas pada anak-anaknya. Memberi apa yang dibutuhkan bagi anaknya untuk berkembang, sesuai apa yang sudah menjadi haknya, untuk menjelajah seisi kota dan dunia, untuk tinggal dan berbuat demi masa yang jauh lebih baik.

Namun apa yang kulihat nyatanya berbeda. Ibuku mengelak saat diajak bicara, ibuku lebih memilih tersenyum pada dunia dan berpaling dari anaknya. Menganggap kita tidak, menganggap kita bukan manusia nyata. Materiku diambil tanpa terasa berguna, aku merasa hampa. Aku merasaבודהā kesempatanku dan penerus bangsa kurasa sudah tidak aku rasa akan lebih dianggap mati sejak lama.

OpenSea/RizkiDut

## Mahasiswa protes, foto rektor ITB dijual sebagai NFT

Liked by **and others**

thefineryreport Dua foto rektor Institut Teknologi Bandung (ITB) dijadikan NFT dan dijual di OpenSea oleh mahasiswa yang belum diketahui identitasnya. Dinamai 'Ibu Rektor Tercinta,' deskripsi NFT tersebut berisi kritik tentang perlakuan sang rektor terhadap mahasiswa yang dinilai abai.

Salah satu kalimat dari deskripsi tersebut berbunyi, "Ibuku mengelak saat diajak bicara, ibuku lebih memilih tersenyum pada dunia dan berpaling dari anaknya."

211 replies, 694 retweets, 3,149 likes

Kedua NFT tersebut belum terjual sampai saat ini.

Tweet your reply



## Ibu Rektor Tercinta #1

Owned by ITB1920 1.6K views 7 favorites

Highest offer

0.001 (\$4.73)

Make offer

Price History

All Time



No item activity yet

## Ibu Rektor Tercinta #2

Market Summary > Bitcoin

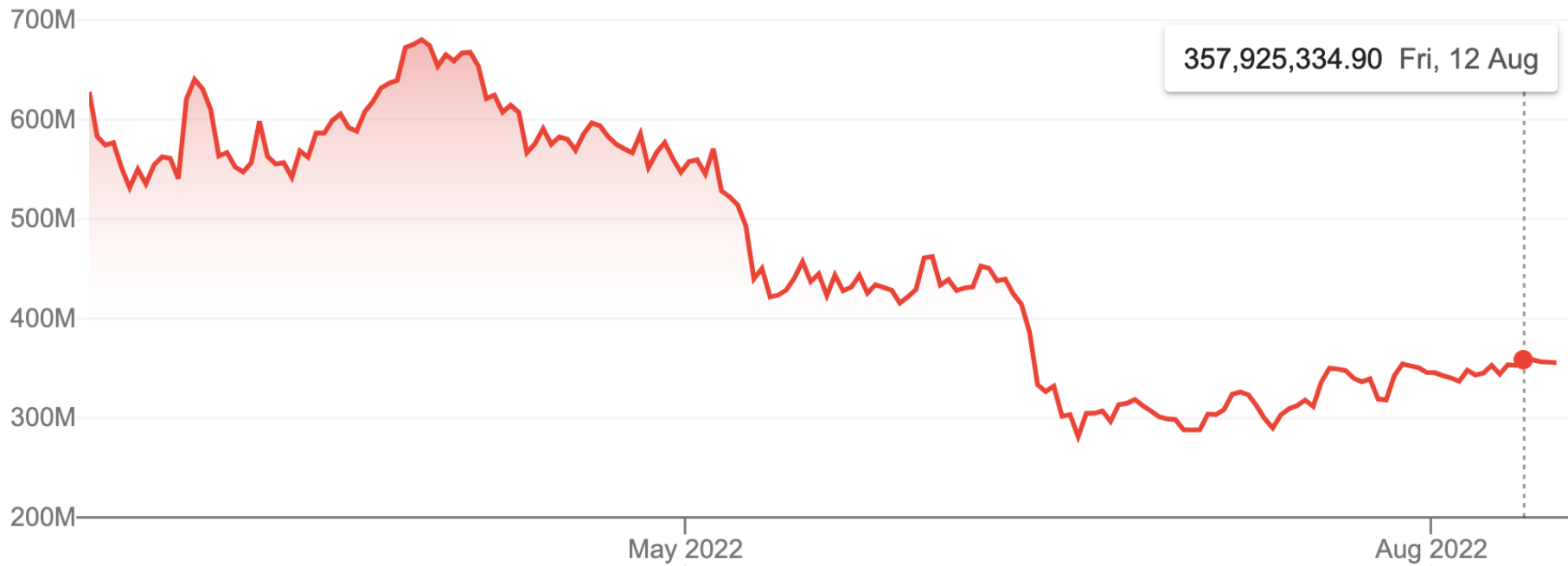
355,597,272.80 IDR

+ Follow

-272,280,105.10 (43.37%) ↓ past 6 months

Aug 16, 11:50 UTC · [Disclaimer](#)

1D | 5D | 1M | **6M** | YTD | 1Y | 5Y | Max

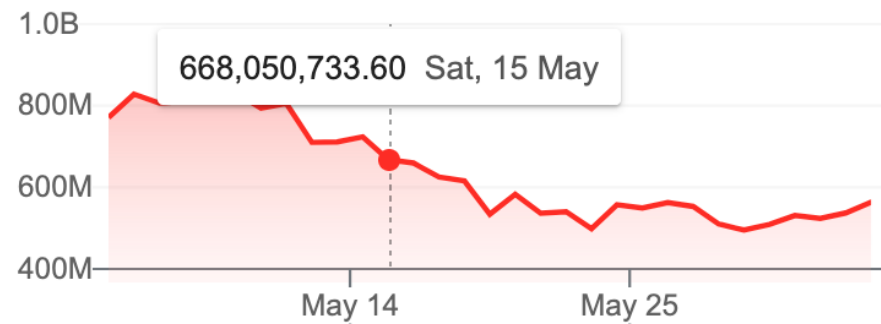


1 Bitcoin equals

# 526,671,902.60 Indonesian Rupiah

Jun 4, 07:03 UTC · Disclaimer

1D 5D **1M** 1Y 5Y Max



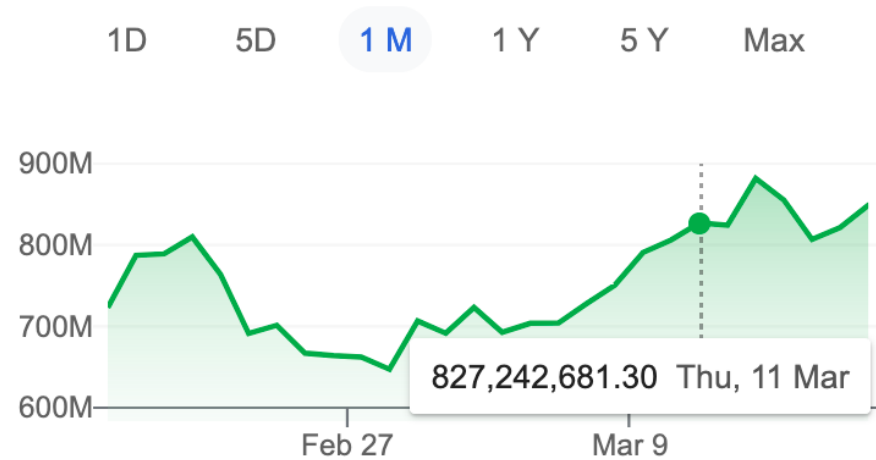
Data provided by Morningstar for Currency and Coinbase for Cryptocurrency

1 Bitcoin equals

# 839,873,730.40

## Indonesian Rupiah

Mar 18, 11:52 UTC · Disclaimer



Data provided by Morningstar for Currency and Coinbase for Cryptocurrency

# Blockchain ≠ Bitcoin









who is satoshi nakamoto



Satoshi Nakamoto is the pseudonym of the person or group of people who created the cryptocurrency, Bitcoin. The true identity of Nakamoto is not known, and it is one of the biggest mysteries in the world of technology and finance. Some people believe that Nakamoto is a single person, while others believe that it is a group of people who worked together to create Bitcoin.

# Blockchain is **Distributed Ledger** Technology

# Ledger

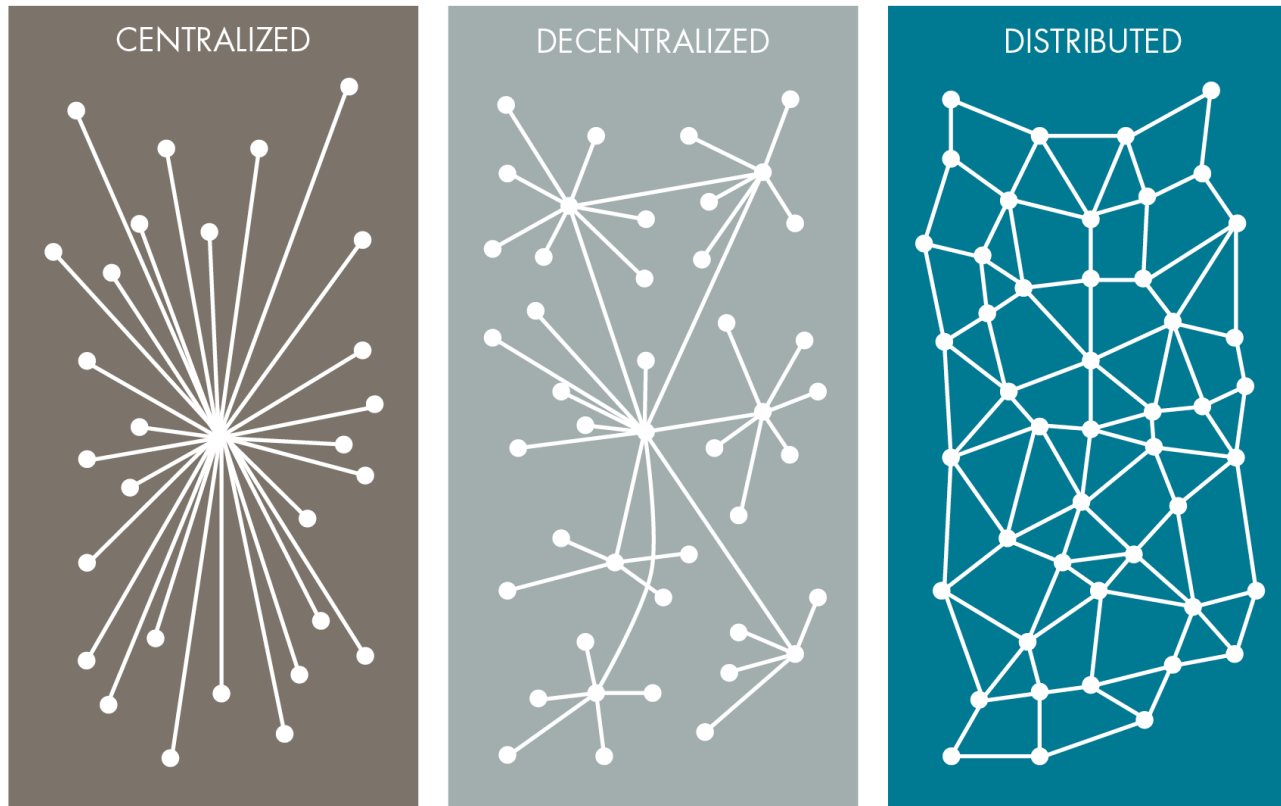
## Definition

- a book or other collection of financial accounts of a particular type
- any kinds of notes

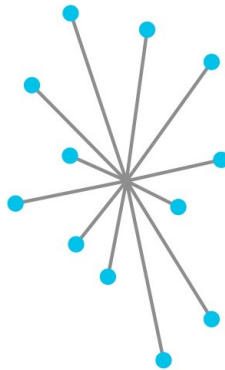
*Accounting Ledger* *Sheet Number:*

No:	Date	Account	Memo	Debit	Credit	Balance	
1							
2							
3							
4							
5							
6							
7							
8			<b>LEDGER ACCOUNTING</b>				
9							
10			<b>NOTEBOOK</b>				
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
23							
24							
25							
26							
27							
28							
29							
30							

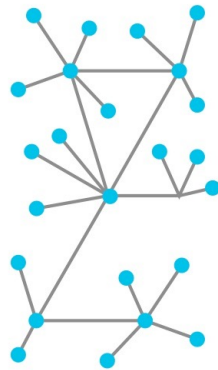
# TYPES OF NETWORKS



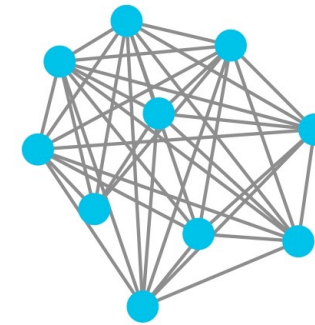
## Centralized



## Decentralized



## Distributed Ledgers



## The New Networks

Distributed ledgers can be public or private and vary in their structure and size.

Public blockchains

Require computer processing power to confirm transactions ("mining")

- Users (●) are anonymous

- Each user has a copy of the ledger and participates in confirming transactions independently

- Users (●) are not anonymous

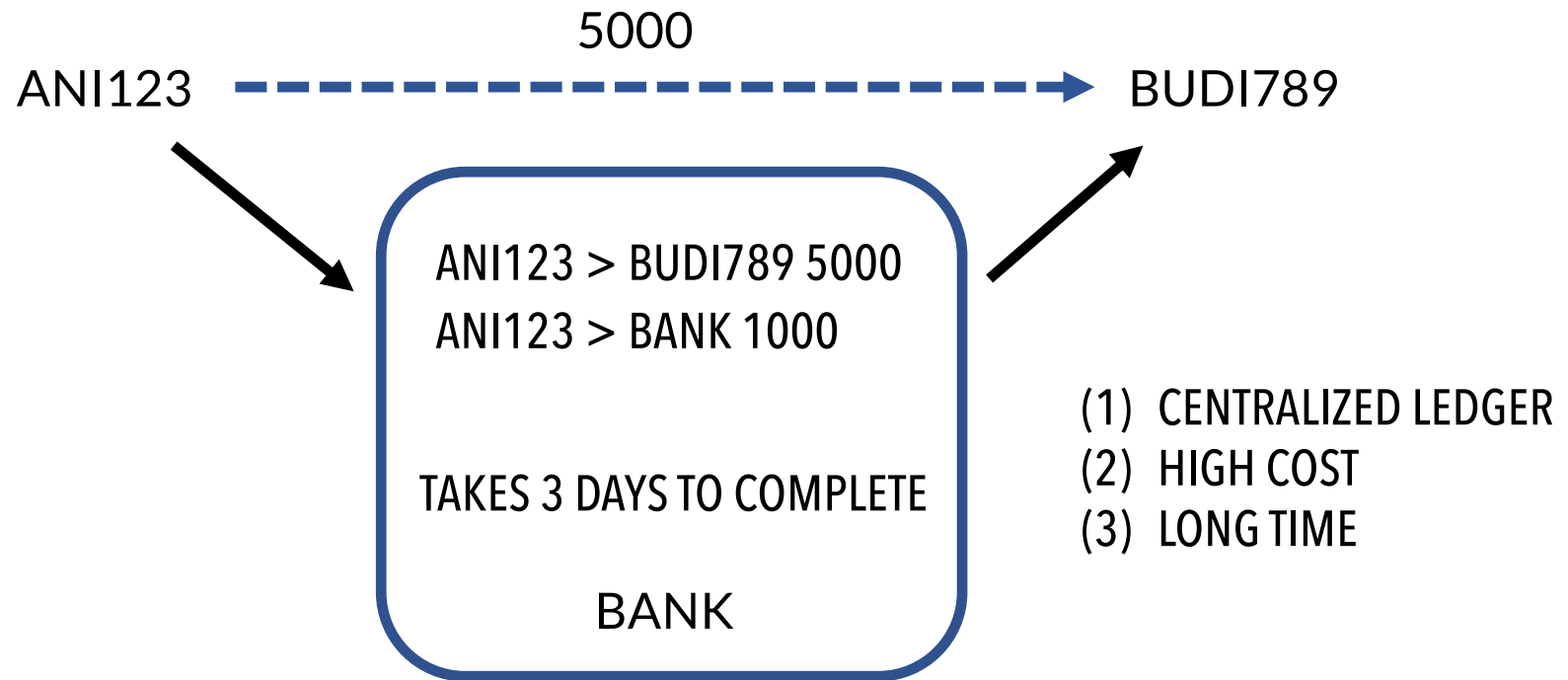
- Permission is required for users to have a copy of the ledger and participate in confirming transactions



# What Problems to Solve?

- Example: conventional banking system
  - Centralized ledger (dependency to a particular entity)
  - High cost
  - Long processing time

# Conventional Transaction





# Conventional Transaction

- Assumption: **ANI123** has balance 1.000.000
- **ANI123** sends 5000 to **BUDI789**
- ANI123 asks 3<sup>rd</sup> party (trusted) such as **bank** as an intermediary
- Bank identifies ANI123 dan BUDI789
- Bank verifies that the transaction is possible (enough fund)
- Bank writes this transaction in its *ledger*
- Bank asks fee for this service
- Bank defines the transaction time
- Everything **depends on the bank**

# Blockchain's Claim

- **Remove** centralized ledger, make it **distributed**
- Create lower transaction fee
- Faster transaction (instant)

# How does it work?

# Hash / Message Digest

- Summary of text / message / stream of data
- One way function that creates signature of data
  - Easy to compute (in forward direction)
  - Difficult (impossible) to compute the inverse
- One bit change will change the output (hash) drastically
- Used to guarantee integrity

# Simple Hash Function

- Message: BUDI .... **RUDI, 292? R=82**
- How to guarantee the integrity of the message? Not tampered

No	Karakter	ASCII
1	B	66
2	U	85
3	D	68
4	I	73
	HASH	$66+85+68+73 = 292$

# Modification Attack | Integrity Check

- RUDI, 292 ???
- $RUDI = 82+85+68+73 = 308$
- attack detected

# Hash Collision

- What is a “collision”?
  - When two different data result in the same hash value
  - From our previous example: BUDI = IDUB
  - $292 = 66+85+68+73 = 67+84+68+73$  (CTDI)
- Hash function must have a low probability of collision
- Examples of good hash function: MD5, SHA256

# Example of Hash usage

- Transaction:

**ANI123 BUDI789 15000**

- Hash (MD5) of that transaction

**34d5853c02351999525194d0c9a69345**

- Hash (SHA-256) of that transaction (note: longer)

**f40ce0a90673486c0bb774feda524e0cb0557b0ae5bc6cd5029b6eb6ad1538cd**



# Example of Block #1

	previous hash
<b>ANI123 BUDI789 15000</b>	current transactions
<b>34d5853c02351999525194d0c9a69345</b>	hash of this block (becomes "previous hash" in next block)

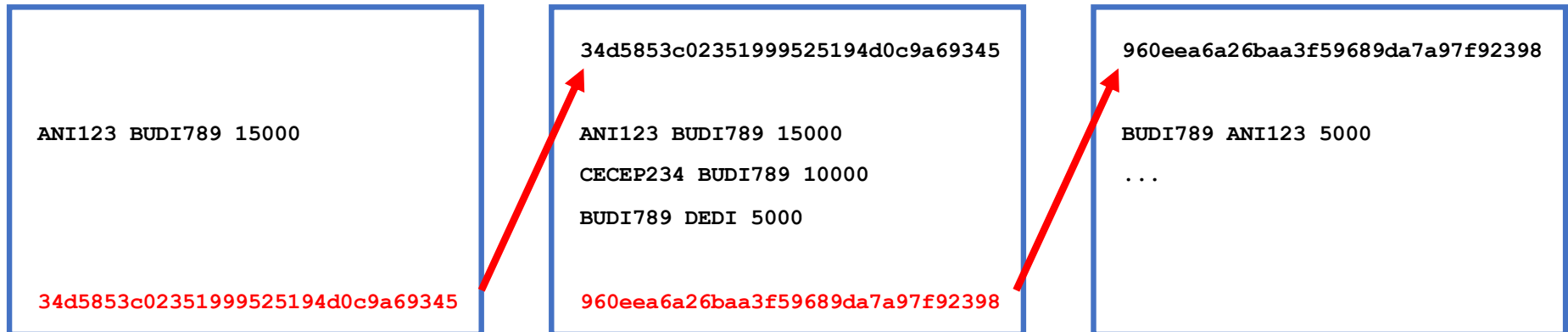
## Example of Block #2

<code>34d5853c02351999525194d0c9a69345</code>	previous hash
<code>ANI123 BUDI789 15000 CECEP234 BUDI789 10000 BUDI789 DEDI 5000</code>	current transactions
<code>41cff38a782117a21817cd493f1958ff</code>	hash of this block (becomes "previous hash" in next block)

# Example of Block #3

<b>41cff38a782117a21817cd493f1958ff</b>	previous hash
<b>BUDI789 ANI123 5000</b> ...	current transactions
	hash of this block (becomes "previous hash" in next block)

# Blockchain = chain of blocks



# Nonce

- Adalah sebuah bilangan atau kata yang kita ambil dari “langit” secara random
- Dalam blockchain, *nonce* digunakan sebagai bagian dari data yang akan di-hash-kan
- Kriteria: cari nilai *hash* tertentu, misalnya nilai *hash* yang paling kecil (ditandai dengan banyaknya jumlah nol di depan angkanya). Ubah-ubah *nonce* sehingga menemukan hash dengan kriteria ini
- Diperebutkan (oleh *miner*). Yang paling dahulu menemukan *nonce* yang menghasilkan hash dengan kriteria tersebut akan diberikan “honor”, *proof of work*

# Nonce

- A random number
- *nonce* will be used as part of data that will be hashed
- Consensus algorithm
  - Find hash that has the **smallest number** (indicated by the number of leading zeros in the number)
  - Change *nonce* to create this hash value
  - The process is called **mining**
- The first “**miner**” that finds this nonce will be declared a winner and will be given a “fee” as a “**proof of work**”

## Example of Block #2 with nonce

<code>34d5853c02351999525194d0c9a69345</code>	previous hash
<code>ANI123 BUDI789 15000 CECEP234 BUDI789 10000 BUDI789 DEDI 5000</code>	current transactions
<code>101010</code>	nonce
<code>000CE9FB2A274F80FFA55C124E206A50</code>	hash of this block (including nonce)

# https://emn178.github.io/online-tools/md5.html

The screenshot shows a web browser window with the URL `https://emn178.github.io/online-tools/md5.html`. The page title is "Online Tools". The main heading is "MD5". Below it, the text "MD5 online hash function" is displayed. A large text input area contains the following text:

```
34d5853c02351999525194d0c9a69345  
ANI123 BUDI789 15000  
CECEP234 BUDI789 10000  
BUDI789 DEDI 5000  
101010
```

Below the input area, there is a dropdown menu for "Input type" set to "Text". A dashed horizontal line separates the input area from the controls. Below the line, there is a "Hash" button and a checked checkbox for "Auto Update". At the bottom, a large text output area displays the MD5 hash:

```
d1caeddbba059ae2de979b47ed8f5c33
```

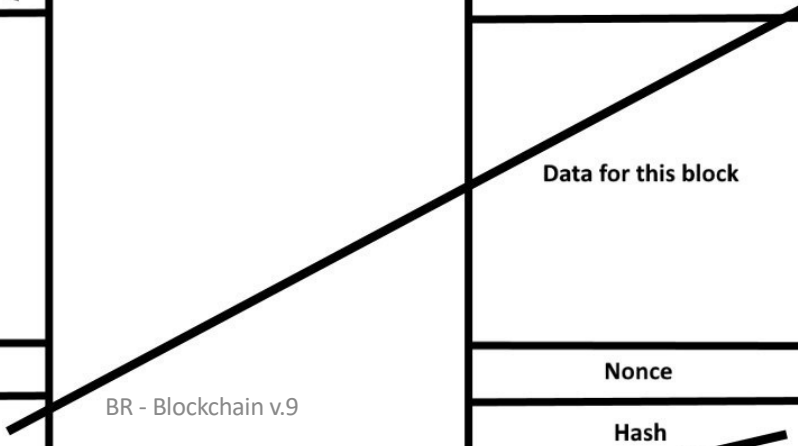
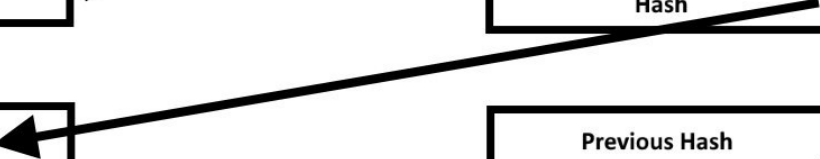
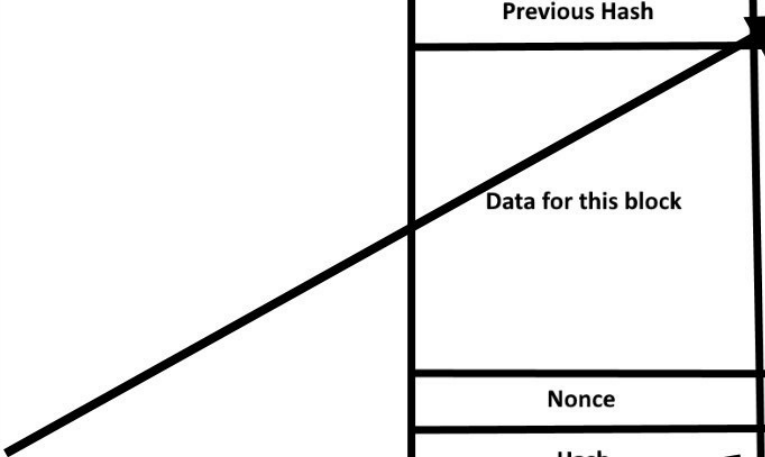
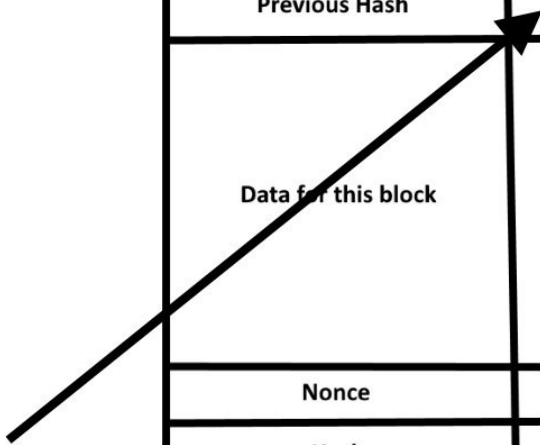


Previous Hash	000012FE....
Data for this block	Date Time Size Transaction Transaction Transaction ...
Nonce	453312
Hash	0000A13465...

Previous Hash	0000A13465...
Data for this block	Date Time Size Transaction Transaction Transaction ...
Nonce	329081
Hash	0000BC34DD...

Previous Hash	0000BC34DD...
Data for this block	Date Time Size Transaction Transaction Transaction ...
Nonce	219988
Hash	0000ADA1B3...

Previous Hash	0000ADA1B3...
Data for this block	Date Time Size Transaction Transaction Transaction ...
Nonce	341123
Hash	0000FE2211...



# Issues

- Many computers are being used to just find ONE nonce
  - Mining is wasting energy. Large amount of electricity is being used
  - Not green
  - Solution: using selected miners
- The number of transactions per second (TPS) is low
  - Because using proof of work
  - Solution: use different kind of consensus

# Mining Alternatives?

---

Proof of Work

---

Proof of History

---

Proof of Stake

---

...

# Smart Contracts

- Instead of just “list of transactions,” we can put code instead
- The code will be distributed and validated
- This code is called “**smart contract**”
- Application examples
  - Buyer put money in smart contract. If product is received, then money is transferred to the seller
  - Kickstarter-like. Supporters put money in smart contracts. If goal is achieved, money is sent to product developer

# Opportunities

# Blockchain-able

- (Business) process that needs distributed ledger
- No trust. No need to have a trusted centralized operator
- **NOT** all processes are blockchainable

# Blockchain Ideas

- Cryptocurrencies
  - DAO (Decentralized Autonomous Organization)
  - DeFi (Decentralized Finance)
  - Electronic voting
  - Electronic marketplace (decentralized ones)
  - IoT (provisioning, data)
  - **NFT** (Non-Fungible Token)
  - Reputation central
  - ...
- Levels
    - Applications
    - Infrastructure
    - Technologies
  - Research examples
    - [next slide]
    - ...

# Research/Initiatives Related to Blockchain

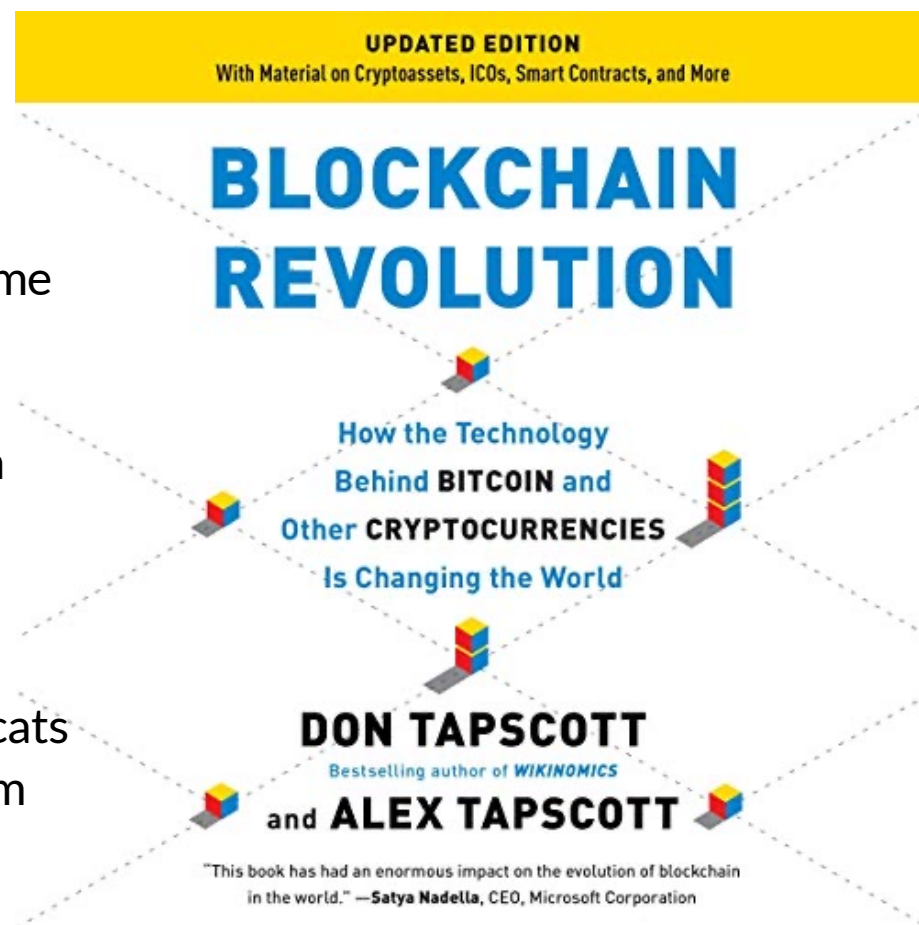
These are a list of partial research that have been done with my students

- e-voting
  - Dwi Fitra Hidayat Satria Wibowo, “Perancangan dan Implementasi Teknologi Blockchain Pada Sistem Pencatatan Hasil Rekapitulasi Pemilu Berdasarkan Formulir C1 Pindaian KPU, Thesis, Februari, 2019
  - e-voting, anonymity, verifiability
- government applications
  - pemantauan penggunaan dana BOS, pertanahan, insurance claims, ...
- coffee tracking
- photo sharing (kios foto)
- traveller helper (help taking pictures, upload photo/video, venue for taking pictures, ... everybody gets a portion of the payment)
- musik: lifetime of a song
- pico payment: digital music store with IDR.P.io
- mobile phone registration, pendaftaran data handphone (IMEI)
- fraud information exchange



# Challenges

1. The technology is not ready for prime time
2. The energy consumed is unsustainable
3. Government will stifle or twist it
4. Powerful incumbents of the old paradigm will usurp it
5. The incentives are inadequate for distributed mass collaboration
6. The blockchain is a job killer
7. Governing the protocols is like herding cats
8. Distributed autonomous agents will form skynet
9. Big brother is (still) watching you
10. Criminals will use it



# How to Implement Blockchain

# Major Platforms

- **Ethereum**  
[www.ethereum.org](http://www.ethereum.org)



- **Hyperledger**  
[www.hyperledger.org](http://www.hyperledger.org)

ethereum **HYPERLEDGER**

- There are “forks” of these two major platforms.
  - J.P. Morgan’s **Quorum**
- Solana
- Others: Tezos, ...
- Indonesia: Vexanium

# Concluding Remarks

- Blockchain technology is a game changer
- The search for **killer application**(s) continues
- (There will be innovations relating to performance, etc.)