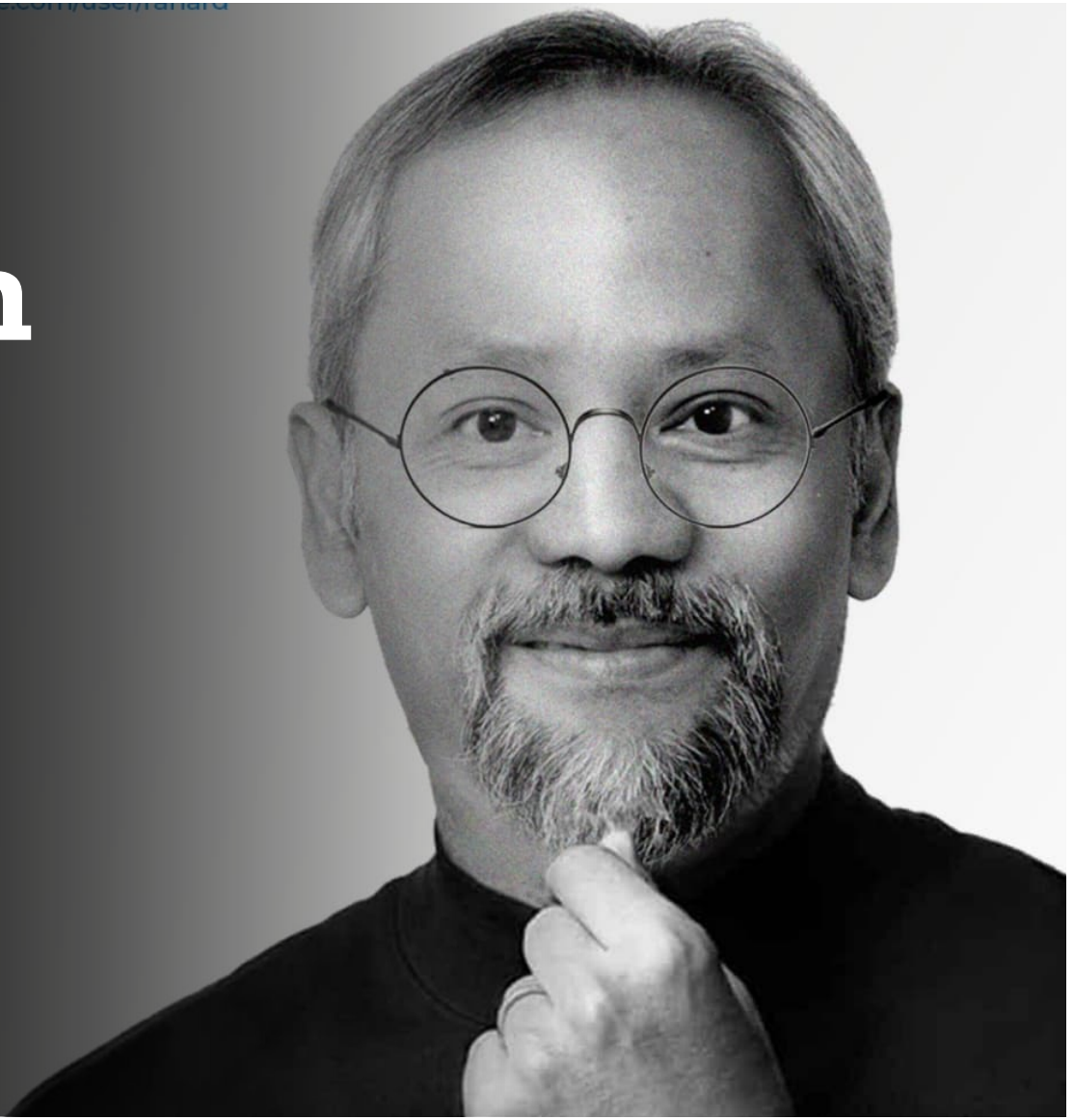
Introduction to Blockchain

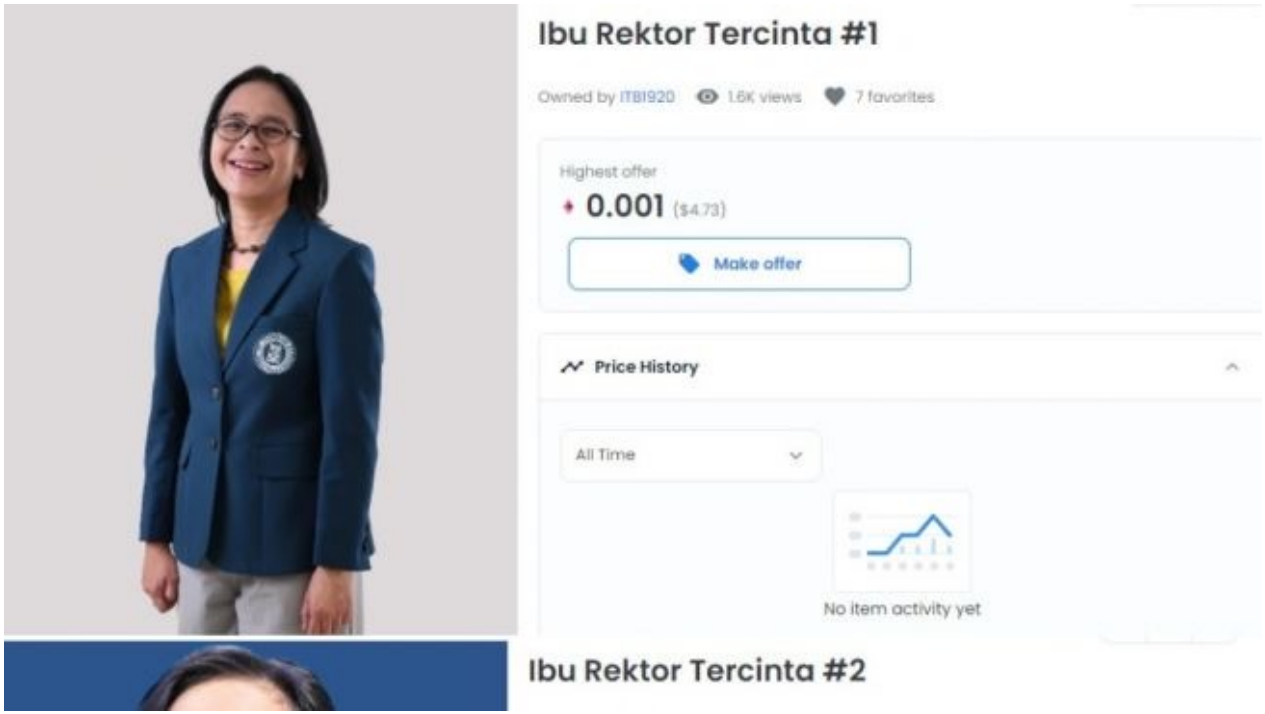
Budi Rahardjo
@rahard
2024



Have you heard of Bitcoin? Cryptocurrency? NFT?


Ghazali NFT

Foto Rektor ITB di-NFT-kan



Market Summary > Bitcoin

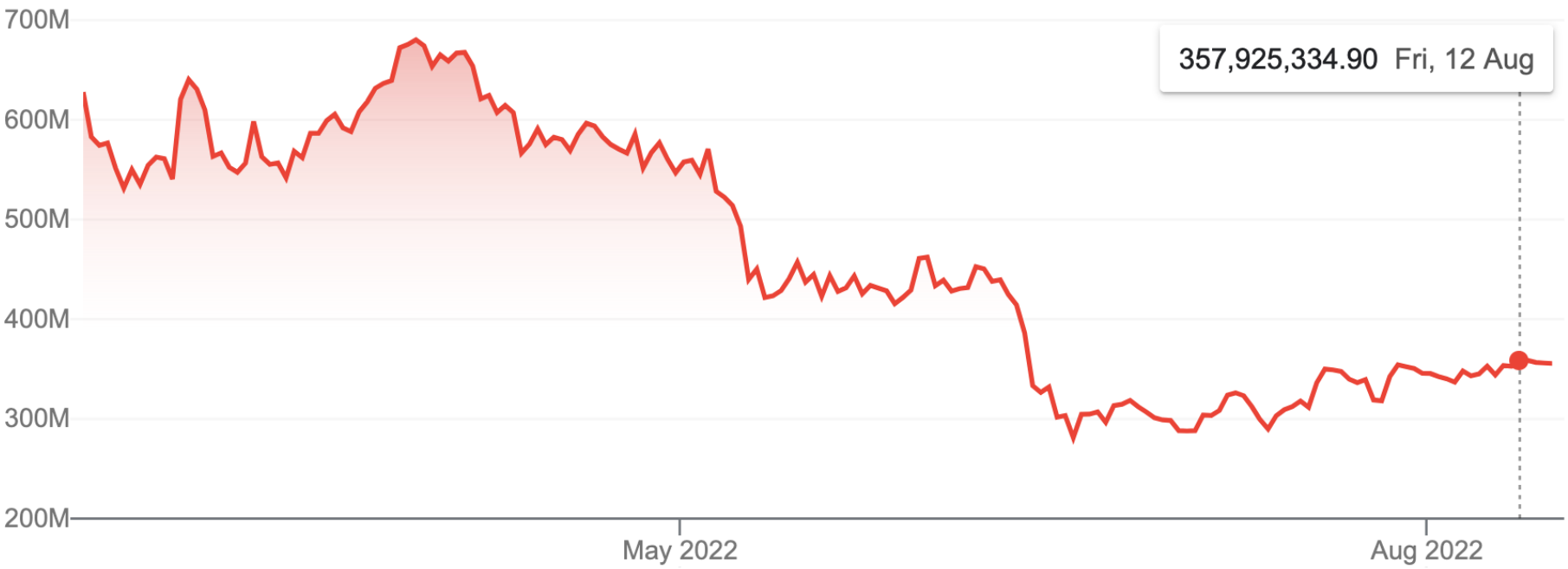
355,597,272.80 IDR

+ 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

1	Bitcoin
526671902.60	Indonesian Rupiah

Data provided by Morningstar for Currency and Coinbase for Cryptocurrency

1 Bitcoin equals

839,873,730.40 Indonesian Rupiah

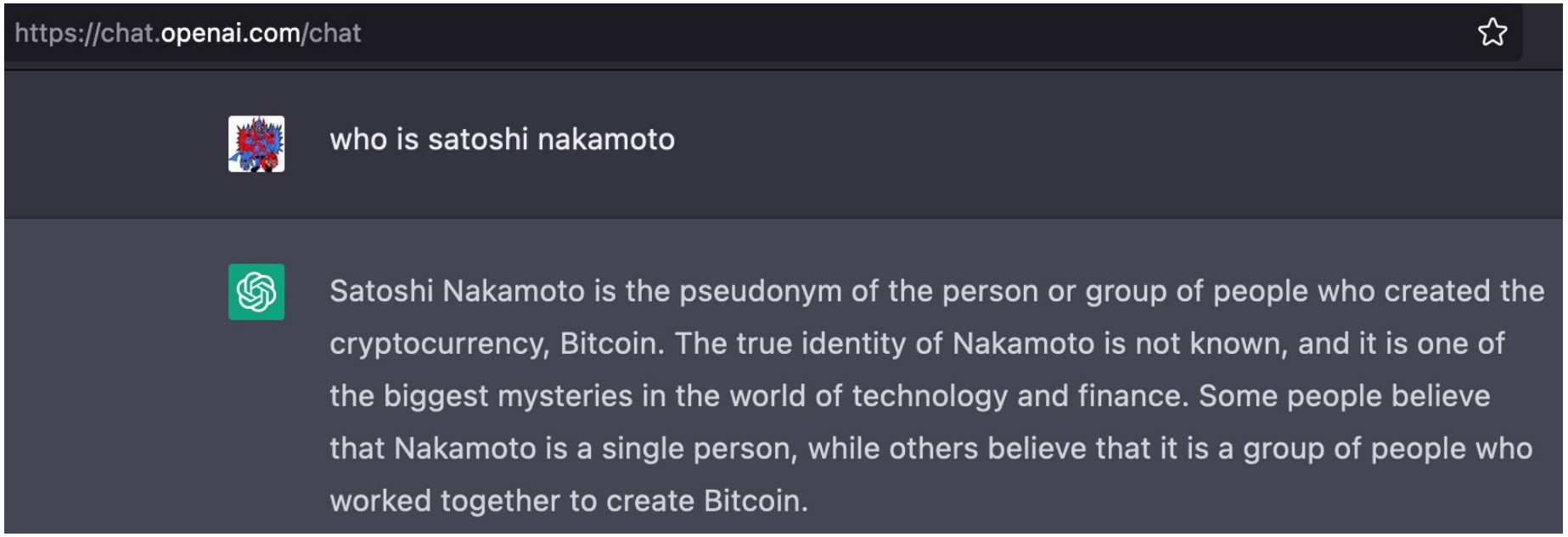
Mar 18, 11:52 UTC · Disclaimer

1	Bitcoin
839873730.40	Indonesian Rupiah

Data provided by Morningstar for Currency and Coinbase for Cryptocurrency

Blockchain ≠ Bitcoin


TIME
MAN OF THE YEAR
Bitcoin Founder
SATOSHI
NAKAMOTO
© CoinedBits.com

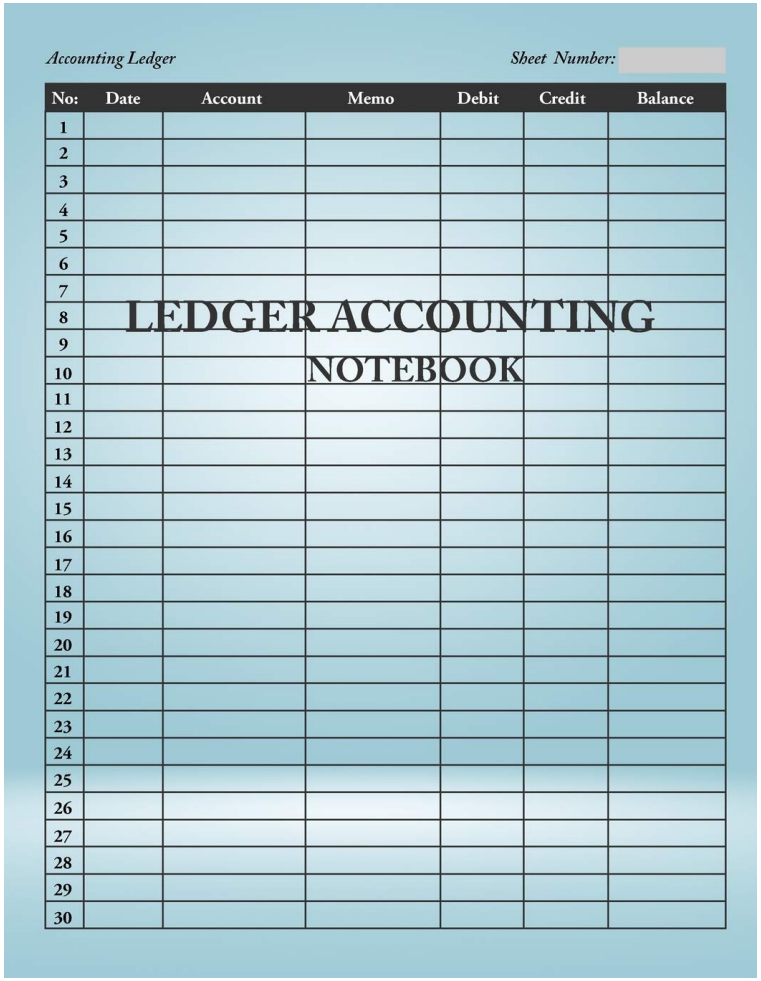

https://chat.openai.com/chat
who is satoshi nakamoto
Satoshi Nakamoto is the pseudonym of the person or group of people who created the cryptocurrency, Bitcoin. The true identity of Nakamoto is not known, and it is one of the biggest mysteries in the world of technology and finance. Some people believe 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

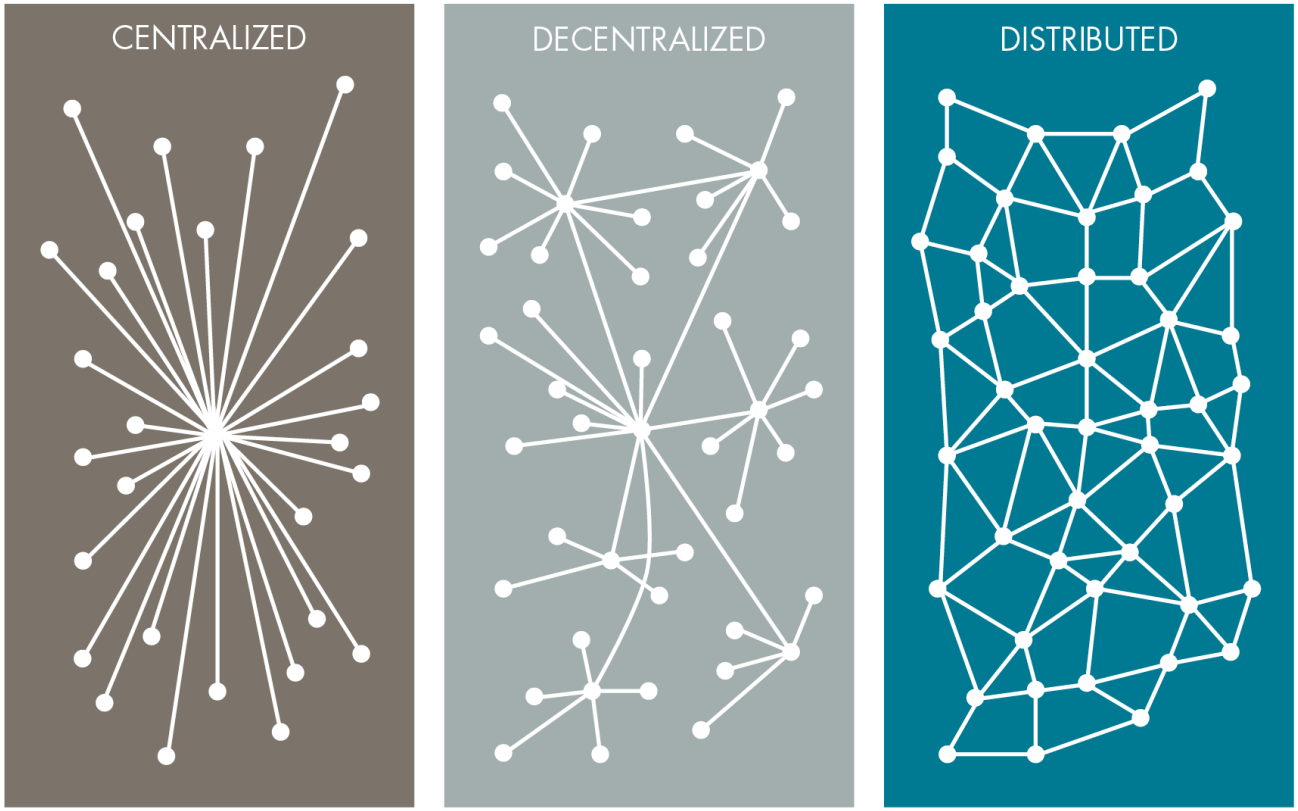
Ledger

Definition

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

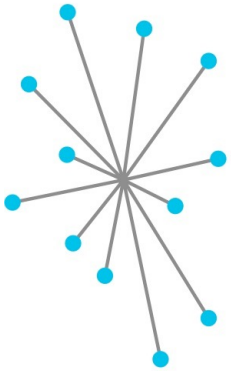


TYPES OF NETWORKS

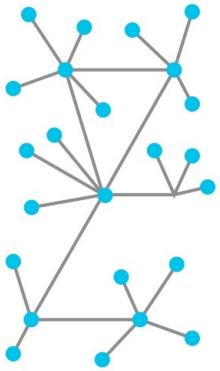


Reproduction of an original figure in "On Distributed Communication Networks" by Paul Baran

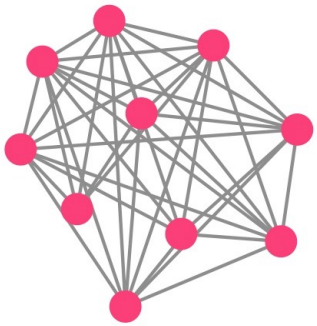
Centralized

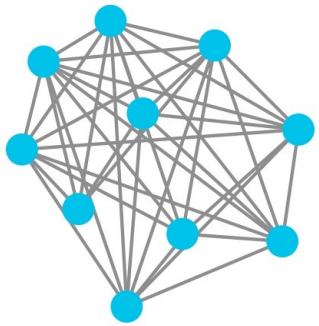


Decentralized



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 legder and partipates in confirming transactions independently

- Users (●) are not anonymous

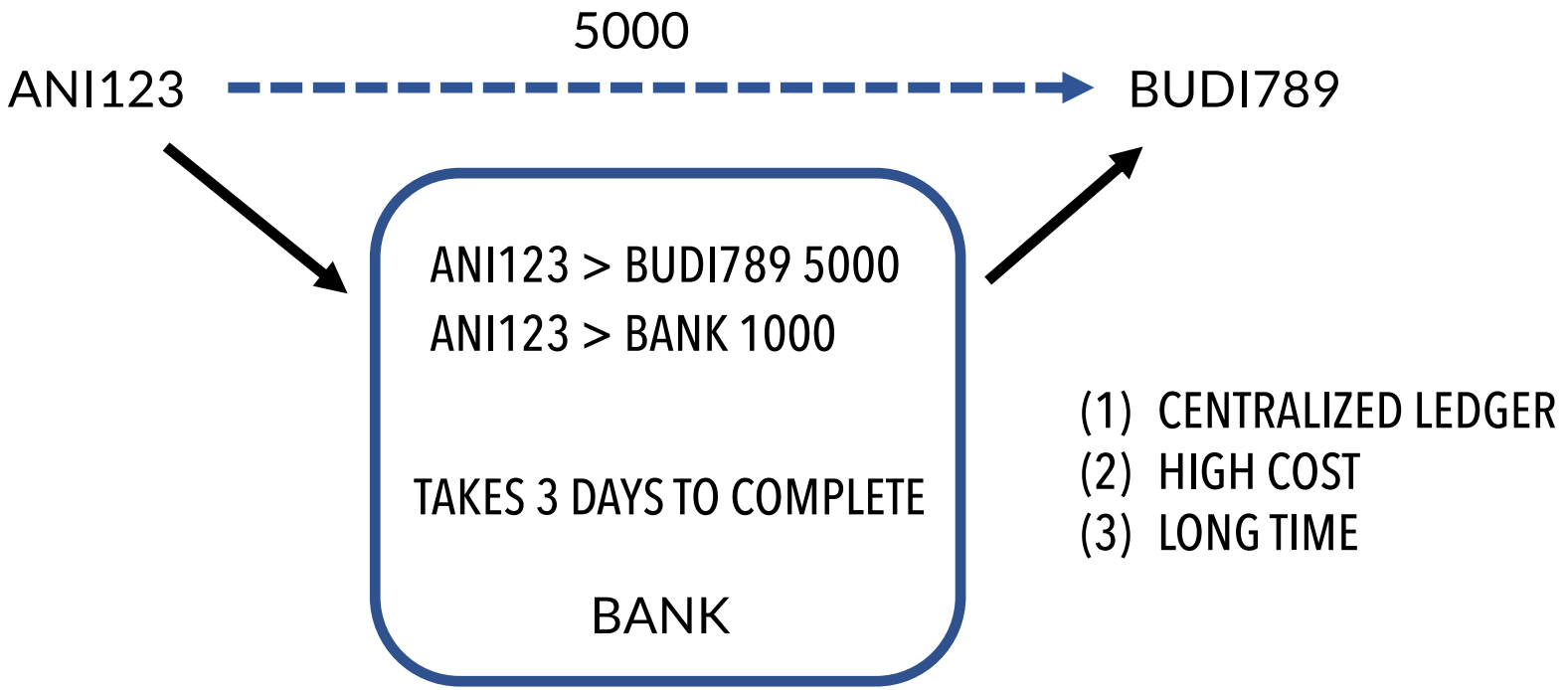
- Permision is required for users to have a copy of the legder and participate in confirming transactions

Blockgeeks

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 3rd 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
```

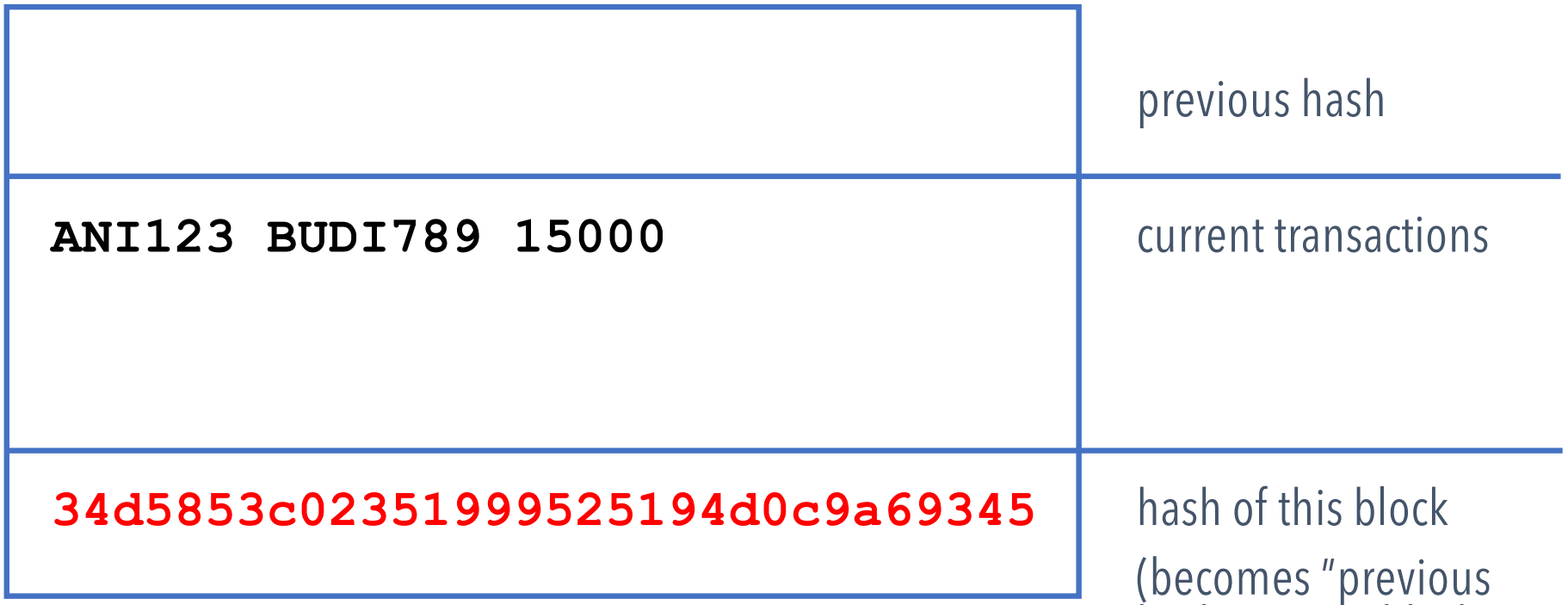
- Hash (MD5) of that transaction

```
34d5853c023519995251 94d0c9a69345
```

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

```
f40ce0a90673486c0bb774feda524e0cb0557b0ae5bc6cd5029b6eb6ad1538cd
```

Example of Block #1



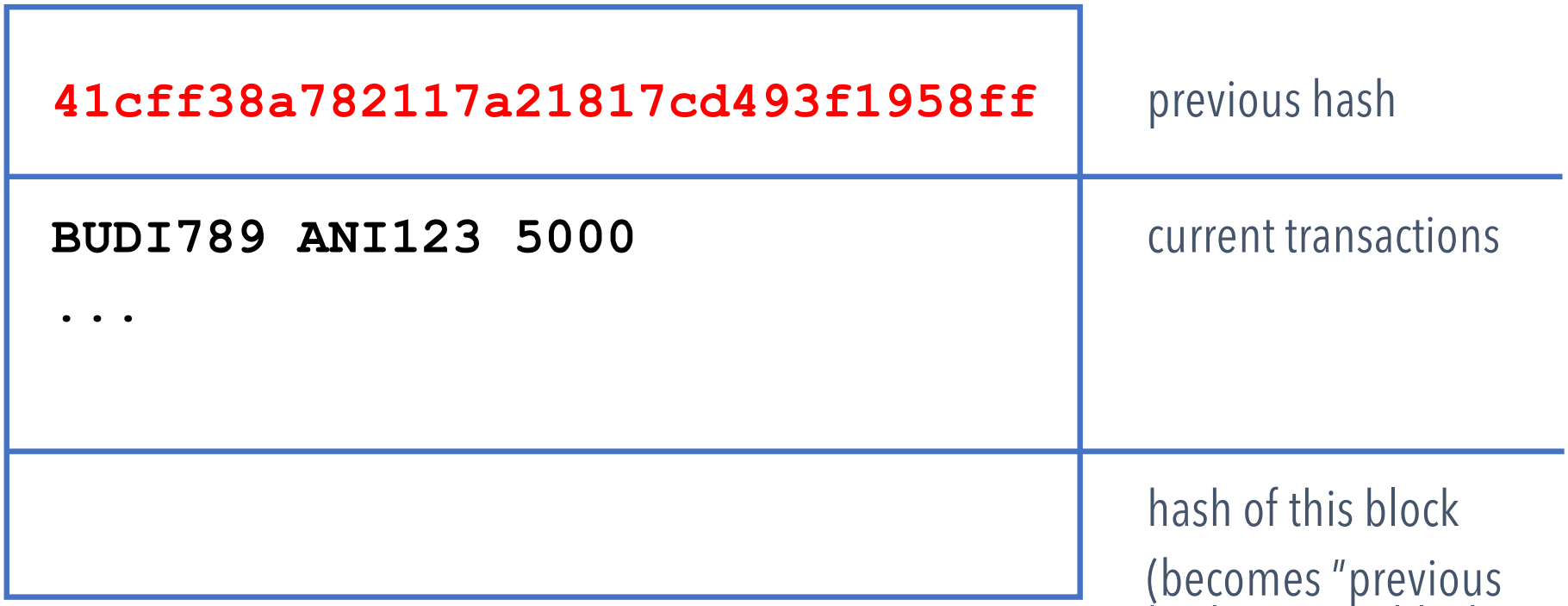
Example of Block #2

`34d5853c02351999525194d0c9a69345`	previous hash

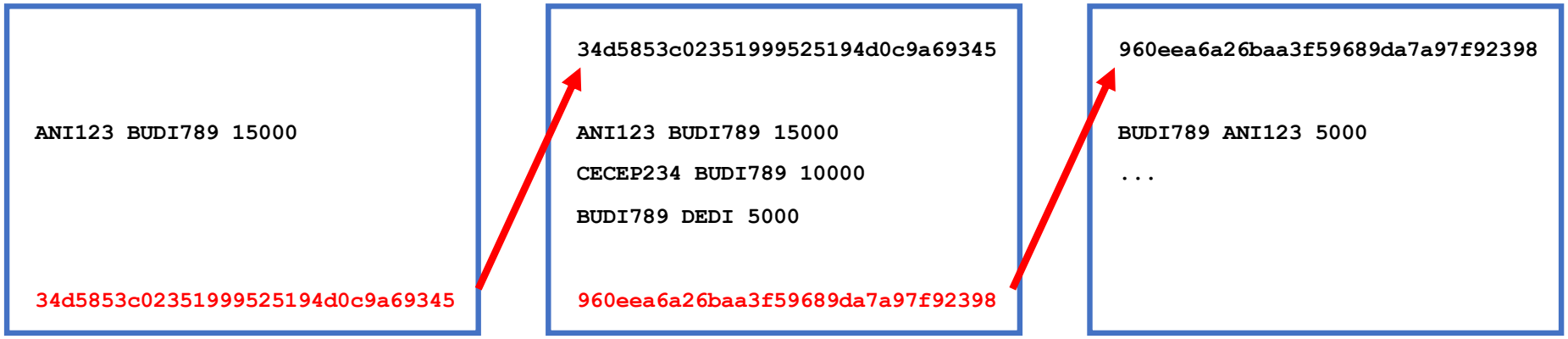
`ANI123 BUDI789 15000`
`CECEP234 BUDI789 10000`
`BUDI789 DEDI 5000`
	current transactions

`41cff38a782117a21817cd493f1958ff`	hash of this block (becomes "previous hash" in next block)

Example of Block #3



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*

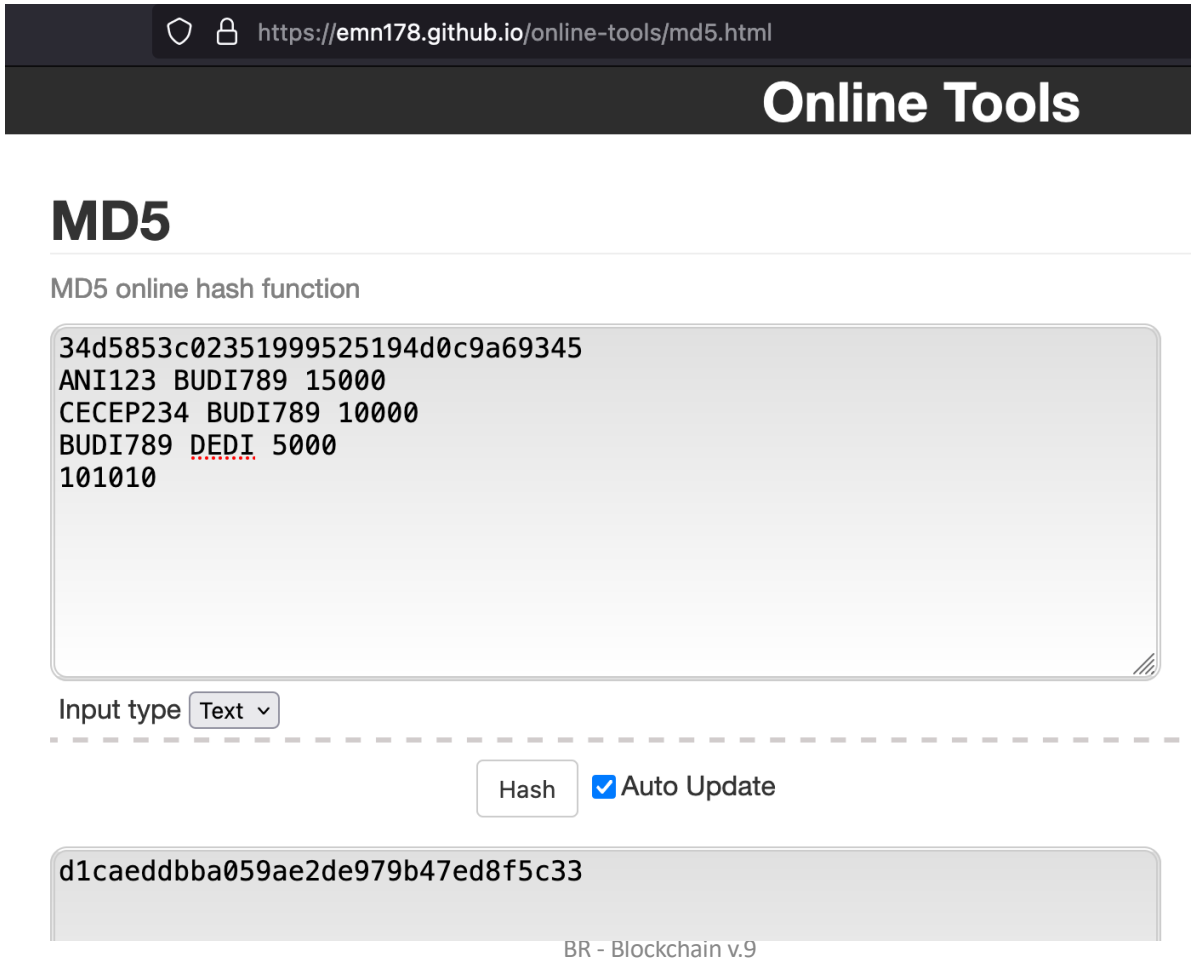
Nonce

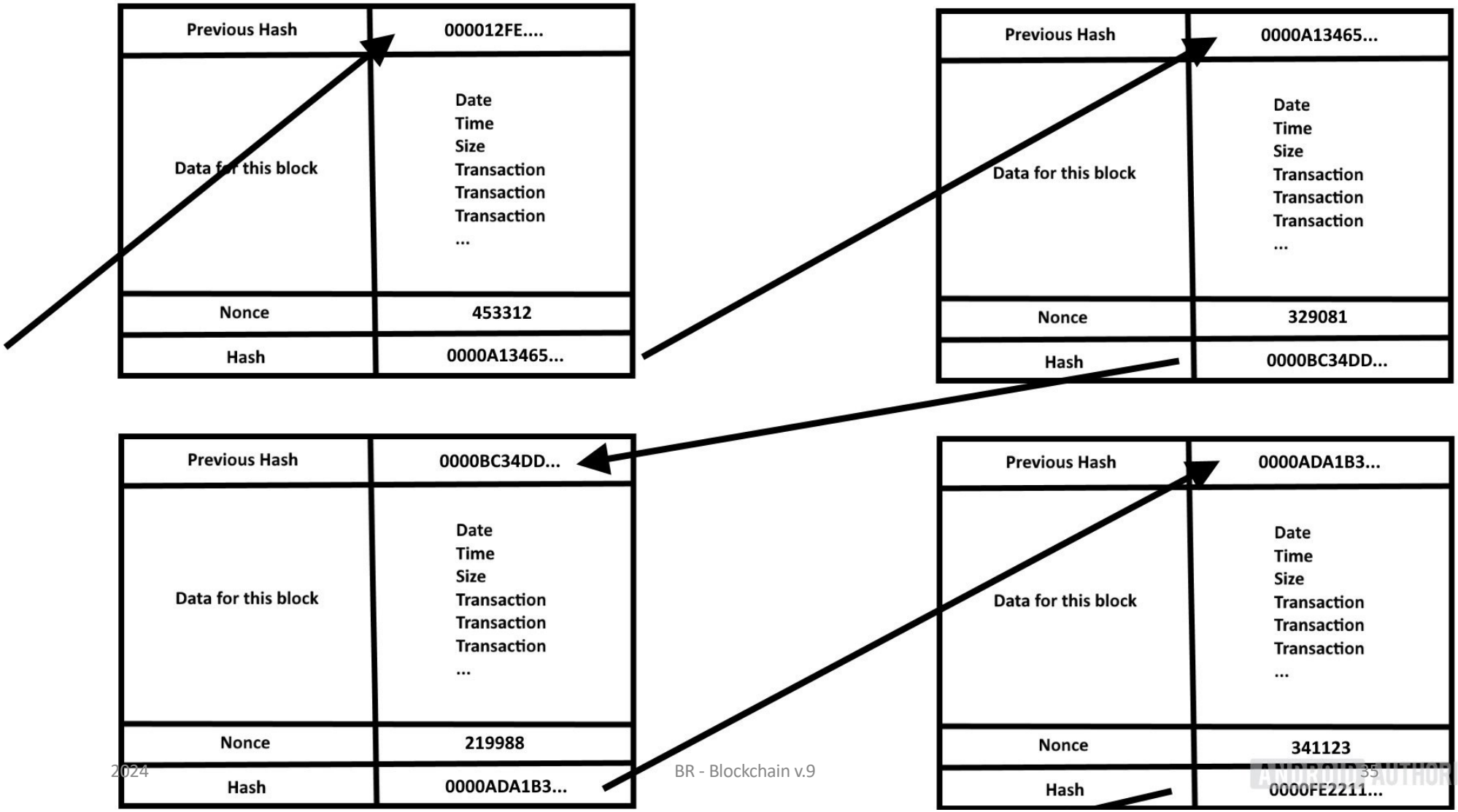
- A random number
- *nonce* will be used as part of data that will be hashed
- Consensus algorithm
  - Find hash that has the **smallest number** (indicated by the number of leading zeros in the number)
  - Change *nonce* to create this hash value
  - The process is called **mining**
- The first "**miner**" 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

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

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




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 patment)
- musik: lifetime of a song
- pico payment: digital music store with IDRP.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 stifile or twist it
4. Powerful incumbents of the old pardigm will usurp it
5. The incentives are unadequate 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
- **Hyperledger**
  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.)