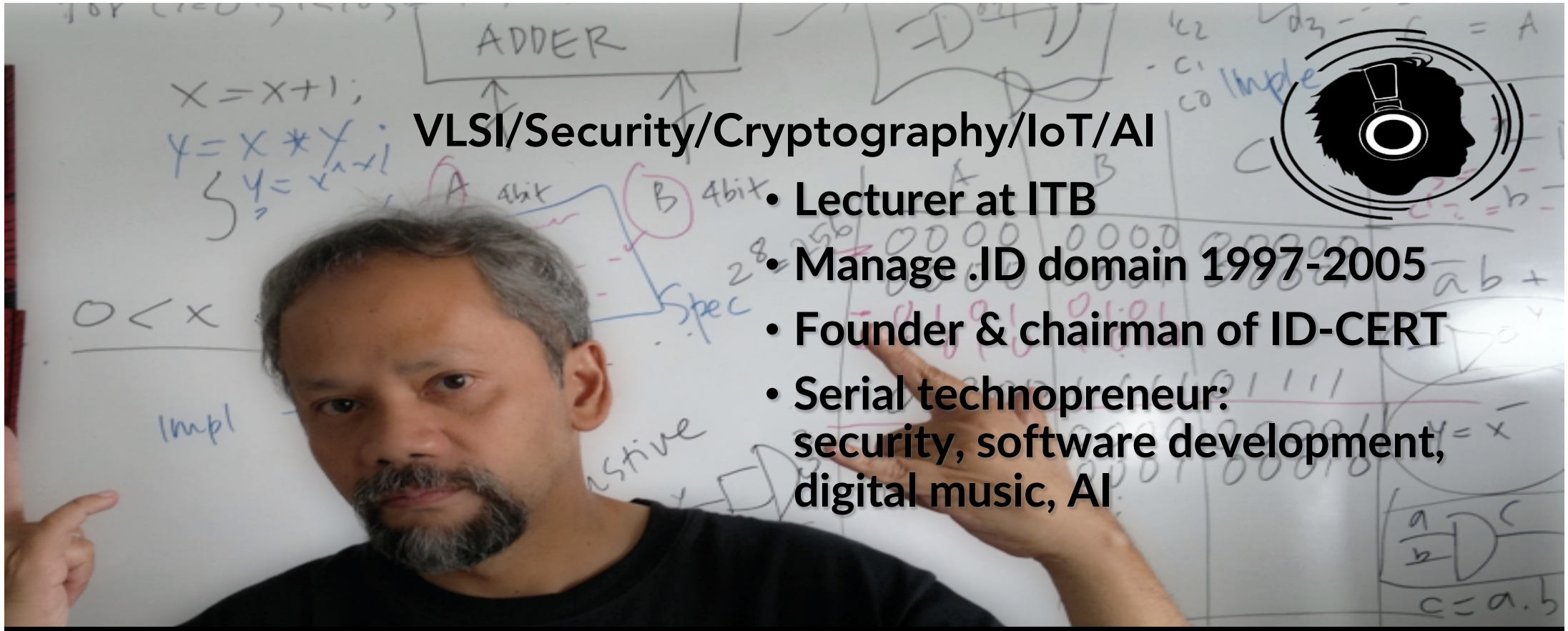
Blockchain Opportunities[?]

Budi Rahardjo

2018

twitter/instagram: @rahard
budi.rahardjo.id
https://github.com/rahard/blockchain



VLSI/Security/Cryptography/IoT/AI

- Lecturer at ITB
- Manage .ID domain 1997-2005
- Founder & chairman of ID-CERT
- Serial technopreneur: security, software development, digital music, AI

id.cert

INDOCISC
NETWORK SECURITY

FOUNDER INSTITUTE

CODE AND RULE THE WORLD

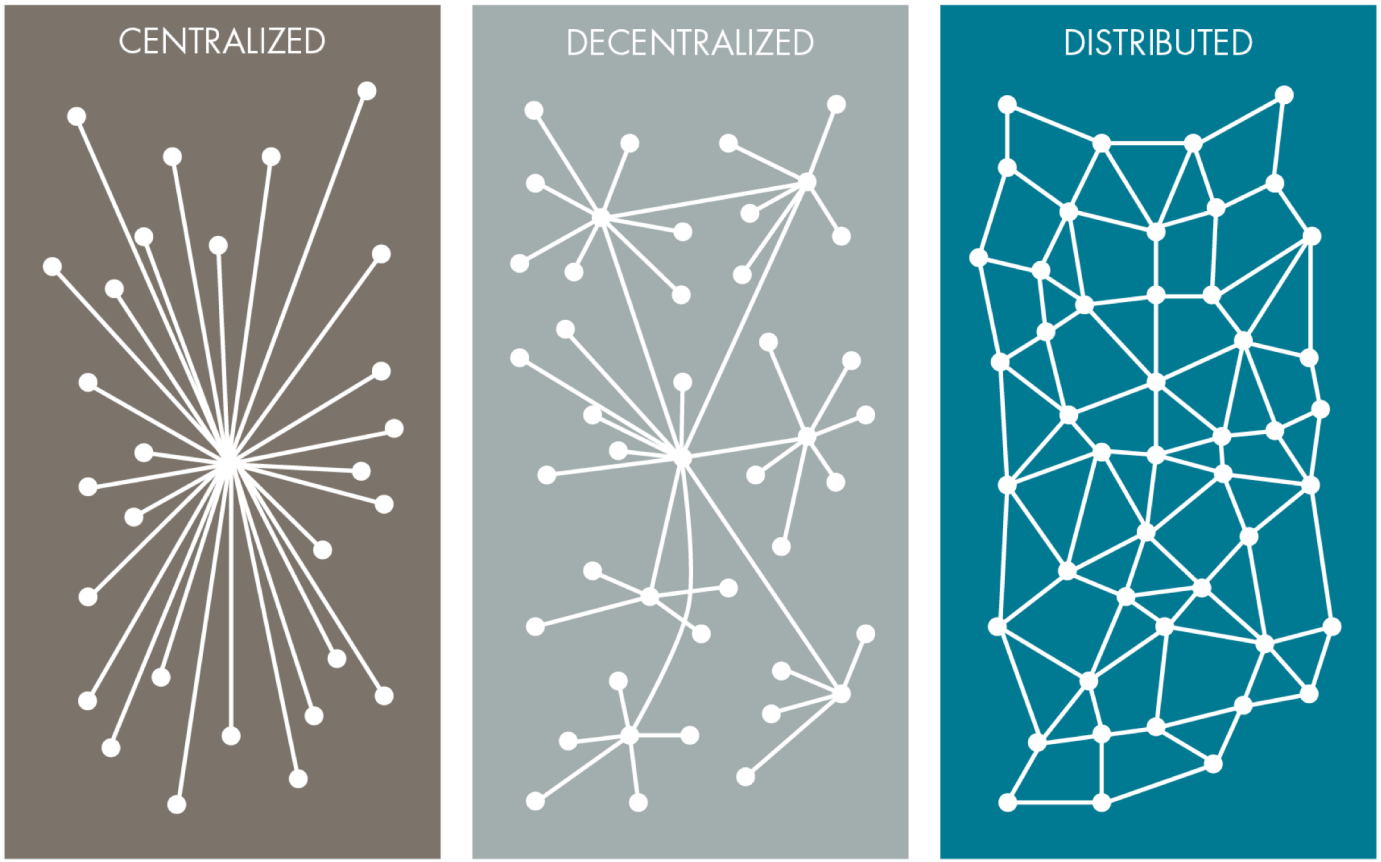
2018 Emerging Technologies

- Internet of Things (IoT)
- Blockchain
- Artificial Intelligence (AI) / Machine Learning / …

Blockchain ≠ Bitcoin


TIME
MAN OF THE YEAR
Bitcoin Founder
SATOSHI
NAKAMOTO
BITCOIN
VIS IN NUMERIS
© CoinedBits.com

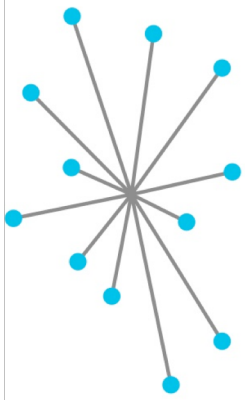
TYPES OF NETWORKS



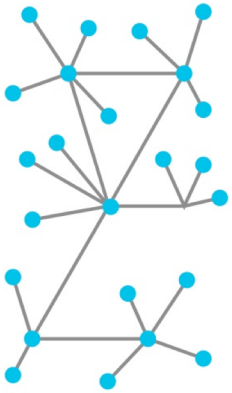
Reproduction of an original figure in "On Distributed Communication Networks" by Paul Baran

Center for Global Development

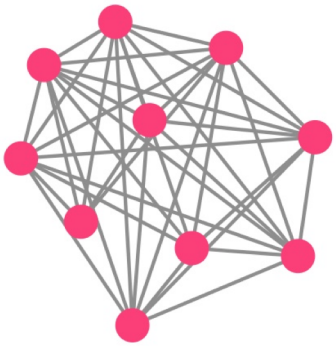
Centralized

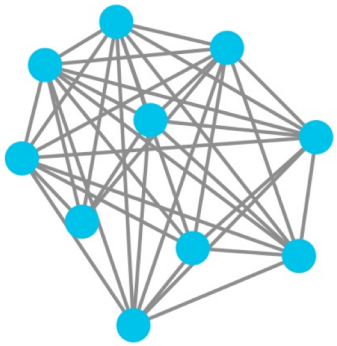


Decentralized



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

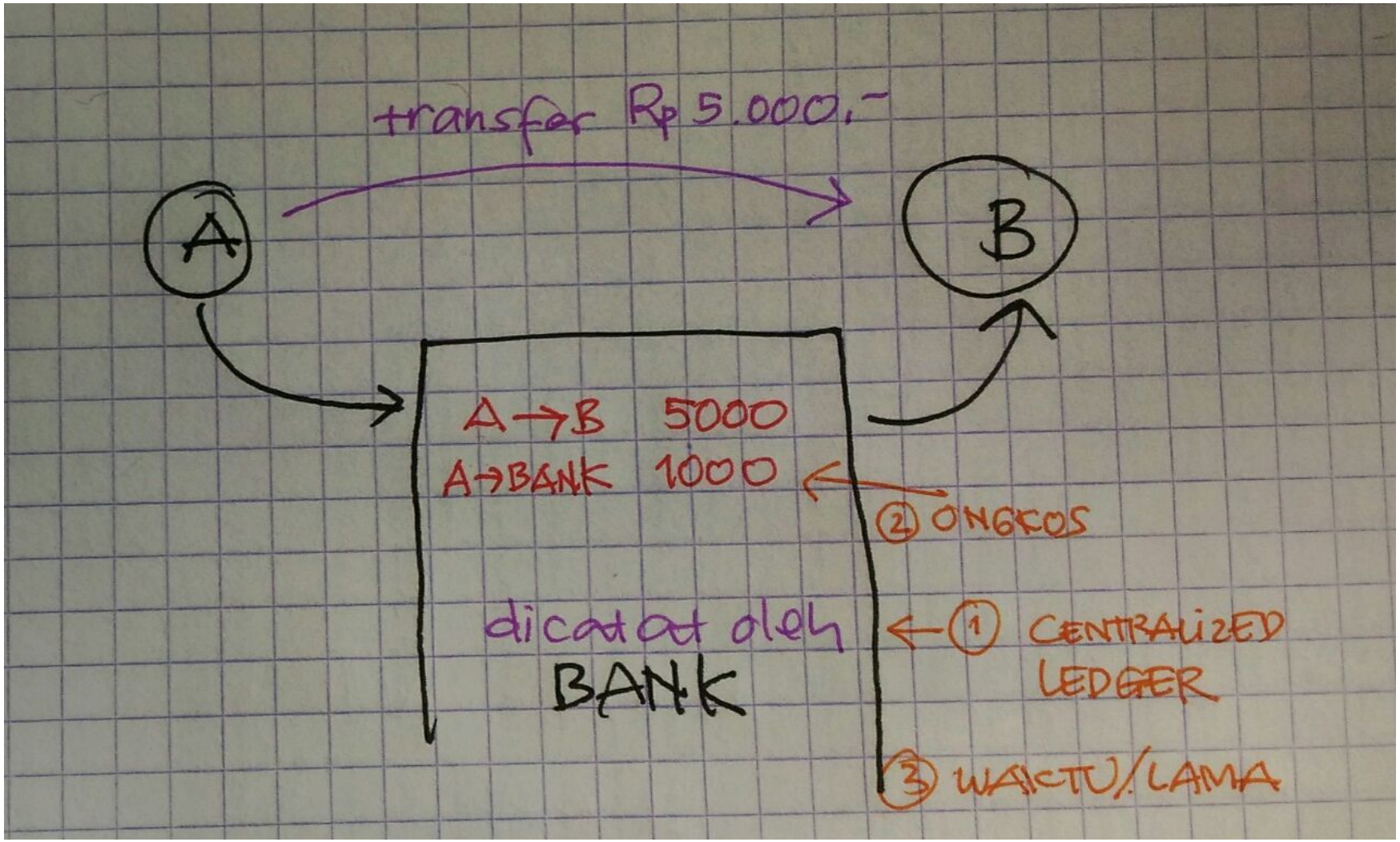
- Permision is required for users to have a copy of the legder and participate in confirming transactions

Blockgeeks

What Problems to Solve?

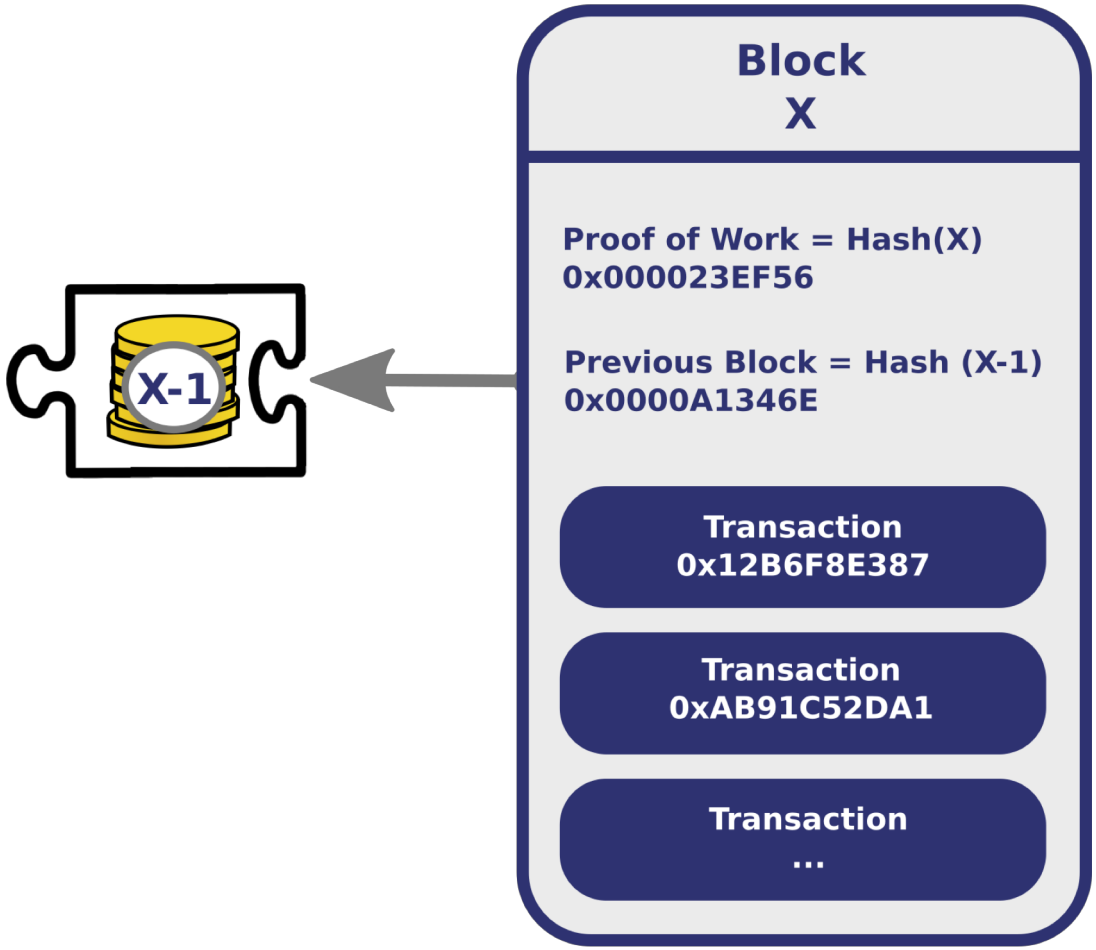
- Centralized ledger (dependency)
- High cost
- Long processing time

Conventional Transaction



Blockchain Technology

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


Block
X
Proof of Work = Hash(X)
0x000023EF56
Previous Block = Hash (X-1)
0x0000A1346E
Transaction
0x12B6F8E387
Transaction
0xAB91C52DA1
Transaction
...
X-1

Hash / Message Digest

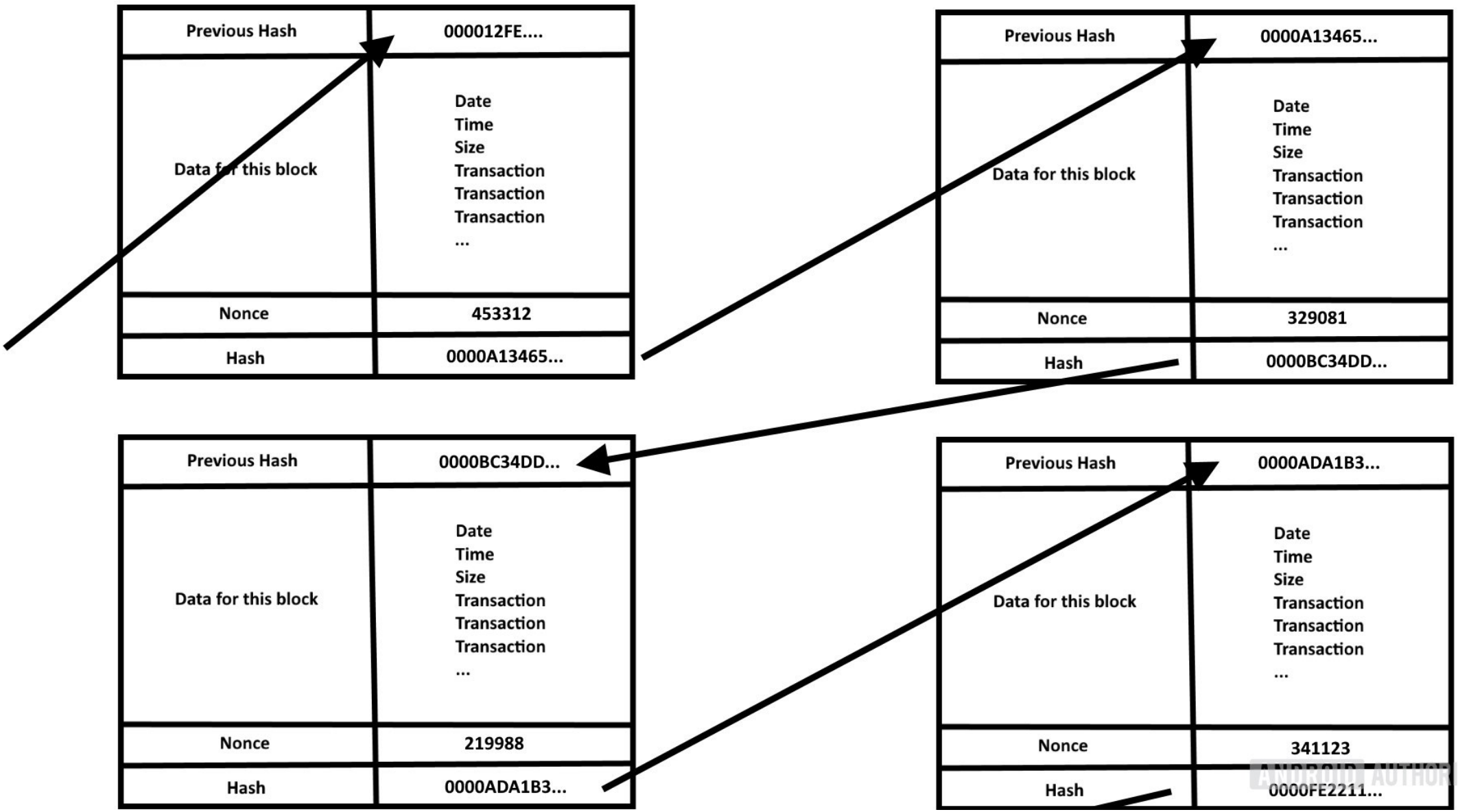
- Merupakan rangkuman dari sebuah pesan / text / message / stream of data
- Merupakan fungsi satu arah (*one way function*) yang dapat menghasilkan ciri (*signature*) dari data (berkas, stream)
  - Mudah dihitung untuk satu arah (forward)
  - Sulit (hard) dihitung inverse-nya
- Perubahan satu bit saja akan mengubah keluaran hash secara drastis
- Digunakan untuk menjamin integritas dan digital signature

Fungsi Hash Sederhana

- Menjumlahkan nilai ASCII dari karakter
- Pesan: BUDI

No	Karakter	ASCII	Total
1	B	66	66
2	U	85	151
3	D	68	219
4	I	73	292

- Adanya masalah dengan collision



Opportunities

Blockchain-able

- (Business) process that needs decentralized ledger
- No trust. No need to have a centralized operator

- **NOT** all blockchainable

Blockchain Ideas

- Electronic voting
- Electronic marketplace (decentralized ones)
- Reputation central
- ...

- Levels
  - Applications
  - Infrastructure
  - Technologies
- Research examples
  - eVoting
  - Asuransi kesehatan
  - Pertanahan
  - Dapodik
  - Handphone curian/selundupan
  - ...

Concluding Remarks

- Blockchain technology is a game changer
- The search for **killer application**(s) continues