Bahan Kuliah II4031 Kriptografi dan Koding

Penggunaan Hash di dalam Blockchain

Oleh:

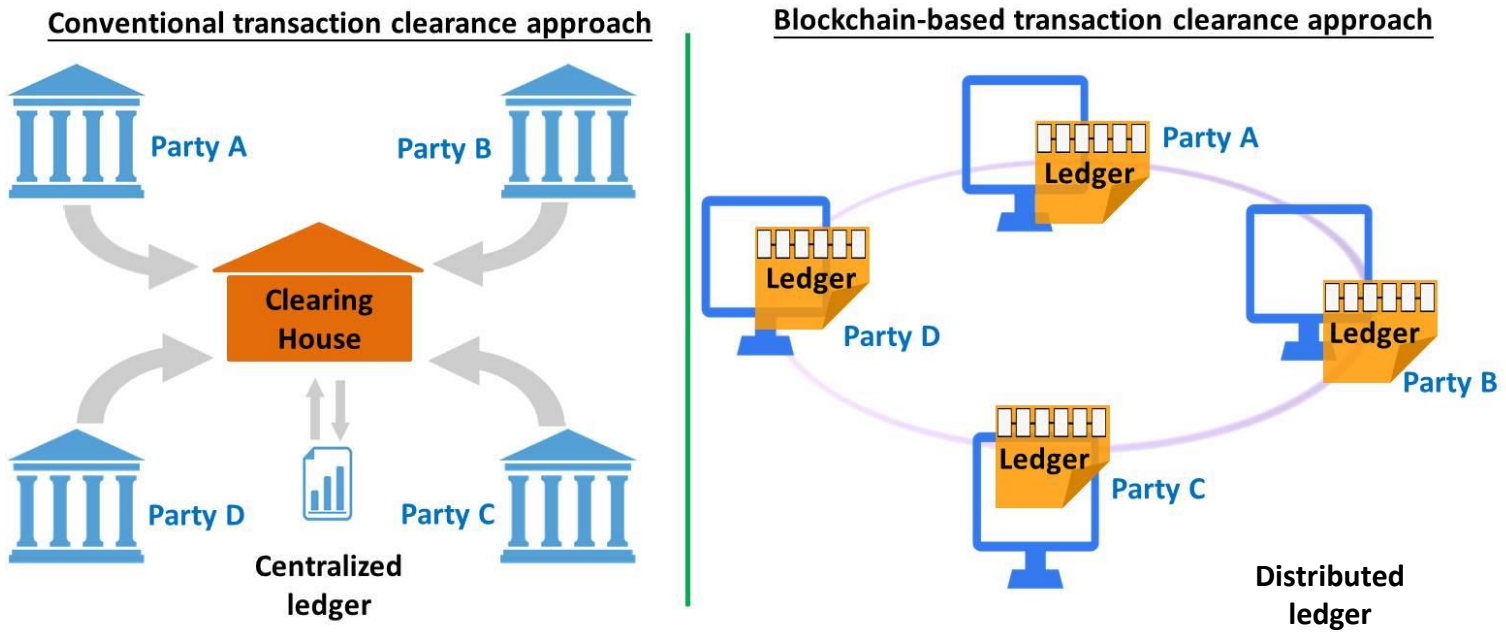
Rinaldi Munir

Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika (STEI)
ITB


BLOCK CHAIN

Blockchain

- *Blockchain* merupakan buku besar (*ledger*) terbuka yang terdesentralisasi (*decentralized*) atau terdistibusi *(distributed ledger)*
- Berbeda dengan pencatatan konvensional yang *centralized* dan membutuhkan pihak ketiga (misalnya bank)



Ledger: Buku yang mencatat transaksi keuangan dalam suatu periode tertentu

BUKU BESAR
(GENERAL LEDGER)

BUKU BESAR
HOTEL PRABU
UNTUK BULAN JUNI 2012

Nama Akun : Piutang Tamu
Kode Akun : 121

Tgl	Uraian	P/R	Debit	Kredit	Saldo
1-Jun	Saldo awal		33000		33000
30-Jun	Jurnal pendapatan	SJ-1	250000		283000
30-Jun	Jurnal penerimaan kas	CR-1		145000	138000

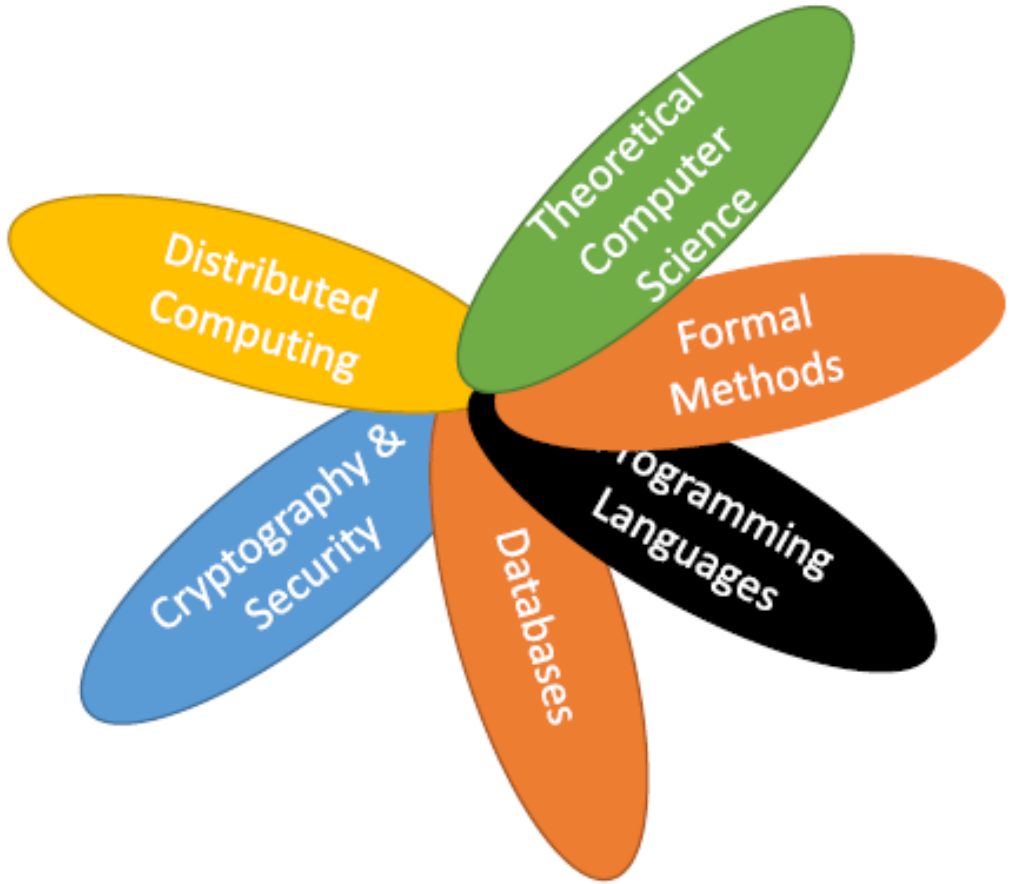
BUKU BESAR

Kode : 11
Nama Akun : Kas
Bulan : 11
Tahun : 2010

Saldo Awal Debet:	0	Mutasi Debet:	9,800,000	Saldo Akhir Debet:	1,820,000
Saldo Awal Kredit:	0	Mutasi Kredit:	7,980,000	Saldo Akhir Kredit:	0

Tanggal	Keterangan	No Ref	Debet	Kredit	Saldo	
					Debet	Kredit
16-Nov-2010	Setoran Modal Awal	101101	4,000,000	0	4,000,000	0
17-Nov-2010	Meminjam uang ke Bank	101102	5,000,000	0	9,000,000	0
18-Nov-2010	Pembelian Kendaraan	101103	0	7,400,000	1,600,000	0
20-Nov-2010	Pembayaran hutang dagang	101105	0	30,000	1,570,000	0
21-Nov-2010	Pendapatan Jasa	101106	800,000	0	2,370,000	0
22-Nov-2010	Biaya-biaya selama sebulan	101107	0	300,000	2,070,000	0
24-Nov-2010	Pembayaran Hutang ke Bank	101109	0	150,000	1,920,000	0
30-Nov-2010	Pengambilan Prive	101110	0	100,000	1,820,000	0
Total			9,800,000	7,980,000		

Bockchain adalah sebuah multidisiplin



Dimana penggunaan hash di dalam blockchain?

Initiation and Broadcasting of Transaction	• *Digital Signatures* • *Private/Public Keys*
Validation of Transaction	• *Proof of Work and certain alternatives*
Chaining Blocks	• *Hash Function*

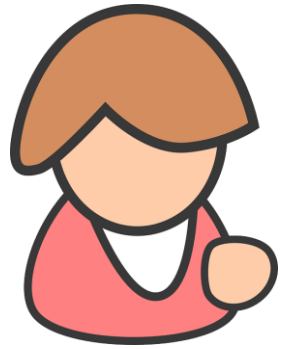
Sumber: “Blockchain at a glance”, I Gusti Bagus Baskara Nugraha, School of Electrical Engineering and Informatics, ITB

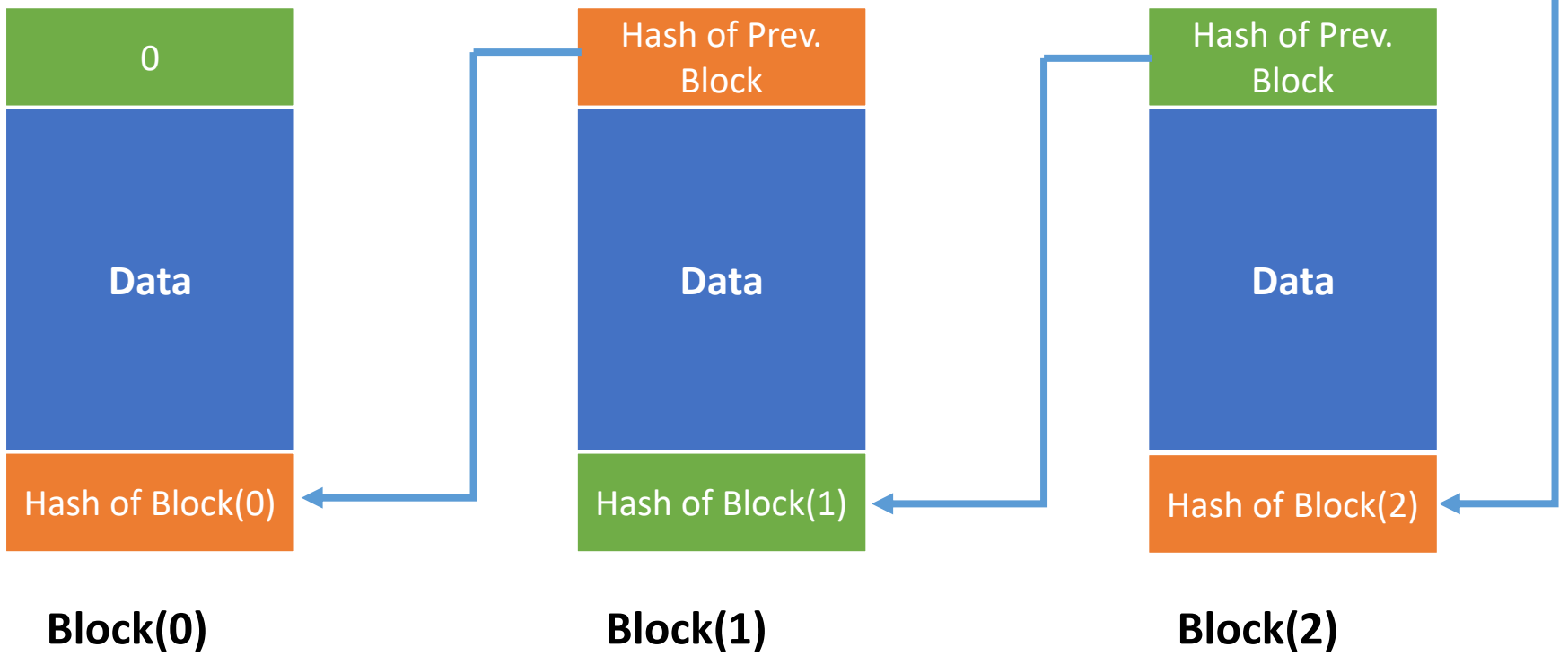
Blockchain

merangkai blok-blok data dengan menggunakan ***hash pointer***

Setiap blok sedikitnya berisi:

- nilai *hash* blok sebelumnya
- nilai *hash* blok ini
- data transaksi





Komponen lebih rinci pada setiap blok:

- A block number
- The hash of the previous block (via this means the 'chain' is being formed)
- Nonce, a random number, see below for more information
- Data: the transactions
- Timestamp with the time the block is created / found
- The hash of the current block

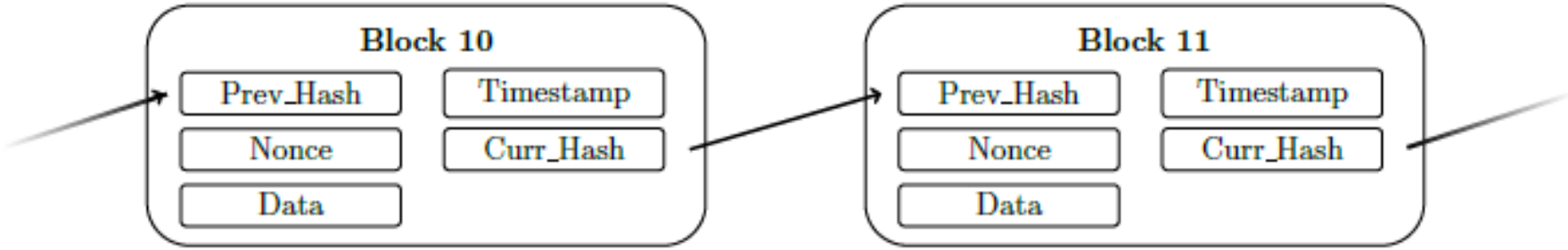


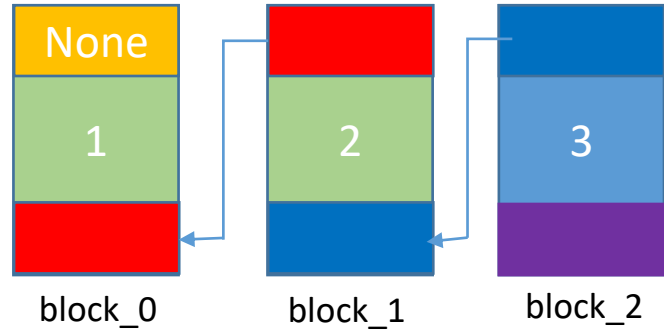
Figure 2.1: Two subsequent blocks in blockchain with their attributes

Program membuat struktur blockchain sederhana dengan Python

```
import hashlib, json
from time import time

block_0 = {
 'prev_hash': None,
 'time' : time(),
 'data': 1,
 'current_hash' : None
}

block_1 = {
 'prev_hash': None,
 'time' : time(),
 'data': 2,
 'current_hash' : None
}
```

```
block_2 = {
 'prev_hash': None,
 'time' : time(),
 'data': 3,
 'current_hash' : None
}

def blockchain(blocks):
  prev_hash = None
  for block in blocks:
     block['prev_hash'] = prev_hash
     block_serialized = json.dumps(block, sort_keys=True).encode('utf-8')
     block_hash = hashlib.sha256(block_serialized).hexdigest()
     block['current_hash'] = block_hash
     prev_hash = block_hash
 return prev_hash

print(blockchain([block_0, block_1, block_2]))
```

runfile('D:/Blockchain/blockchain.py', wdir='D:/Blockchain')
587b5ae6f25ebd88880fd86a7337d63622ae5661a0b9a13b7d21eee1d39613af

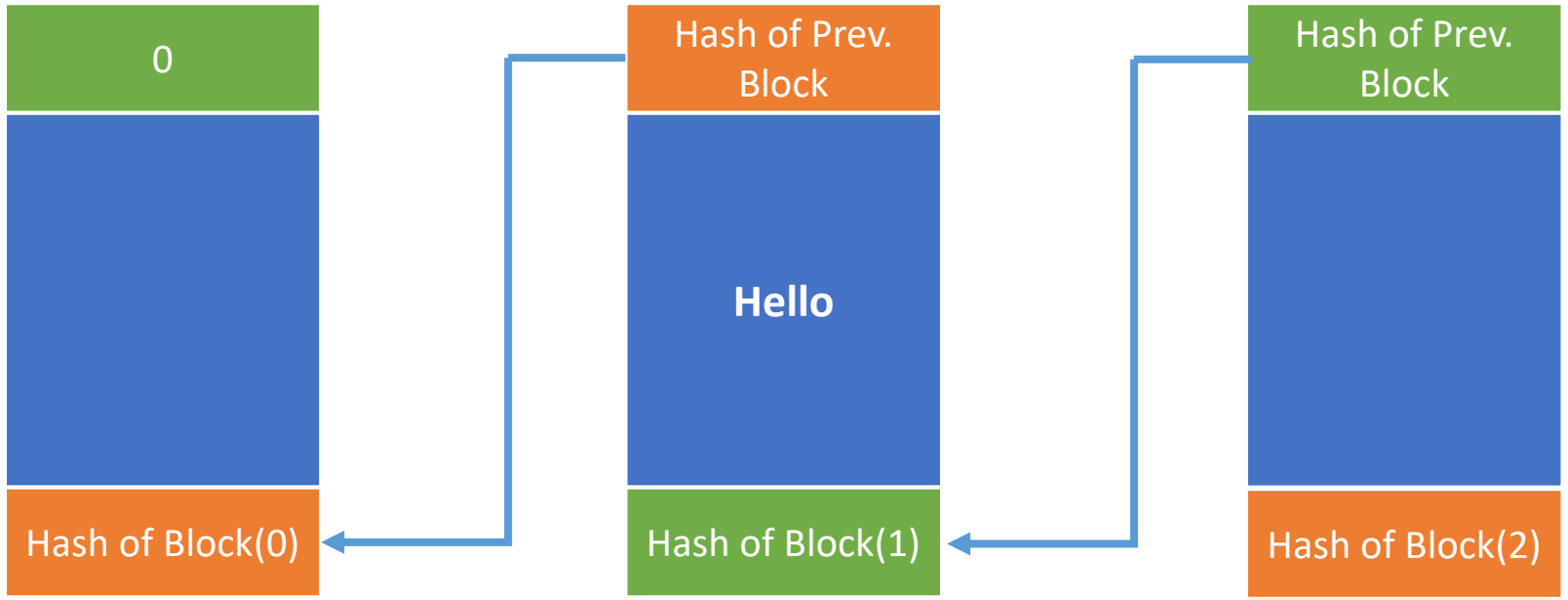


block_0
Out[85]:
{'prev_hash': None, 'time': 1575433243.9058905, 'data': 1,
'current_hash': '05ad2692b90be260734b9fd151a4a471e6d2e06d616831f6efb1fc3e315c411f'}

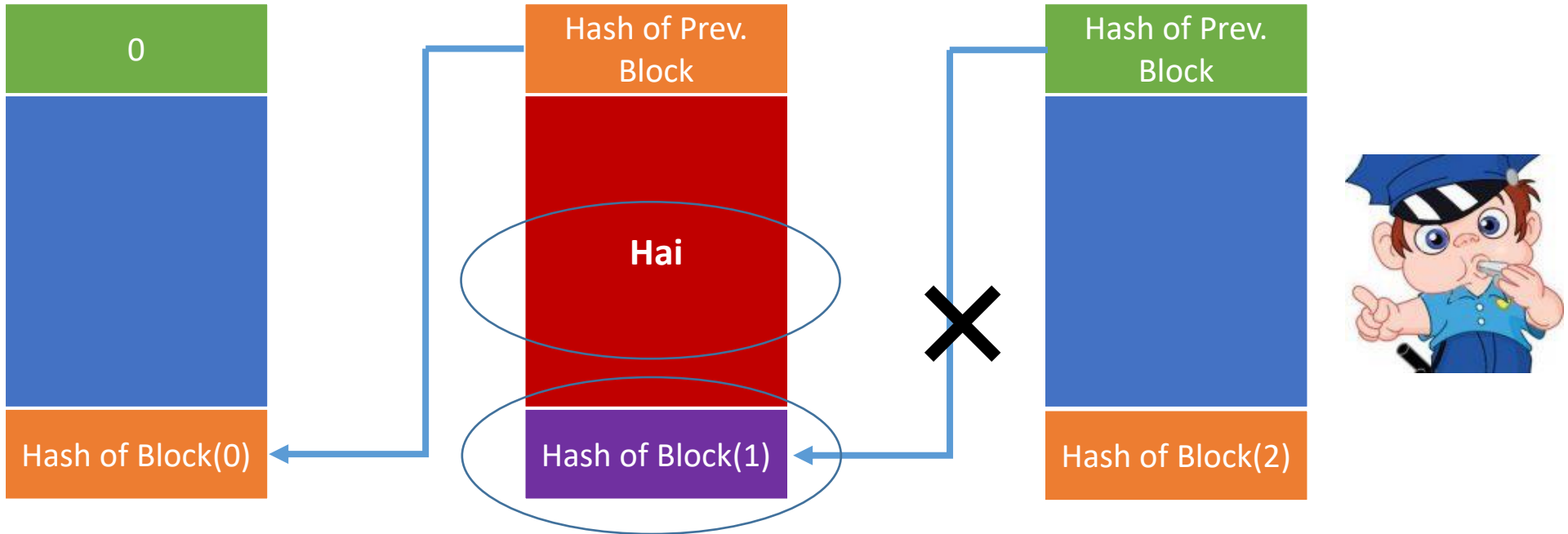
block_1
Out[86]:
{'prev_hash': '05ad2692b90be260734b9fd151a4a471e6d2e06d616831f6efb1fc3e315c411f',
'time': 1575433243.9058905, 'data': 2,
'current_hash': '4c6a3bb0730f6a3ff74b5a54b4f9706d7485ebf932d475440d619155093bac96'}

block_2
Out[87]:
{'prev_hash': '4c6a3bb0730f6a3ff74b5a54b4f9706d7485ebf932d475440d619155093bac96',
'time': 1575433243.9058905, 'data': 3,
'current_hash': '587b5ae6f25ebd88880fd86a7337d63622ae5661a0b9a13b7d21eee1d39613af'}

Data di dalam
blockchain
tidak dapat diubah



Seseorang
mengubah
data Block(1)



Demo *blockchain*:

https://andersbrownworth.com/blockchain

Sifat-sifat *blockchain*

- **Blockchain merupakan sistem yang Transparan**

  Blockchain dikembangkan dengan konsep ***Open-source*** , para developernya membuka *source code*-nya ke publik dan memberikan **dokumentasi**/*white paper* dengan penjelasan yang detail mengenai **cara kerja, protokol dan implementasi** sistem blockchain tersebut.

- **Blockchain bersifat *Decentralized***

  Sistem yang terdesentralisasi **akan lebih baik** dari sistem yang terpusat dalam menghadirkan sebuah sistem pencatatan transaksi yang **transparan** dan **terpercaya**.

- **Blockchain bersifat *Immutable***

  Seluruh block data yang sudah lulus protokol konsensus dan dimasukkan ke dalam blockchain adalah final dan tidak dapat diganggu gugat oleh siapapun, tidak bisa diubah, dimanipulasi.

- **Blockchain bersifat Independent dan Personal**

  Blockchain menghadirkan solusi untuk memungkinkan kita berinteraksi secara langsung dengan aset kita tanpa harus menggunakan pihak ketiga sebagai perantara.

- **Blockchain bersifat *Disruptive*.**

  Teknologi Blockchain adalah sebuah teknologi yang *disruptive*, yang akan mengubah banyak sekali aspek kehidupan umat manusia.

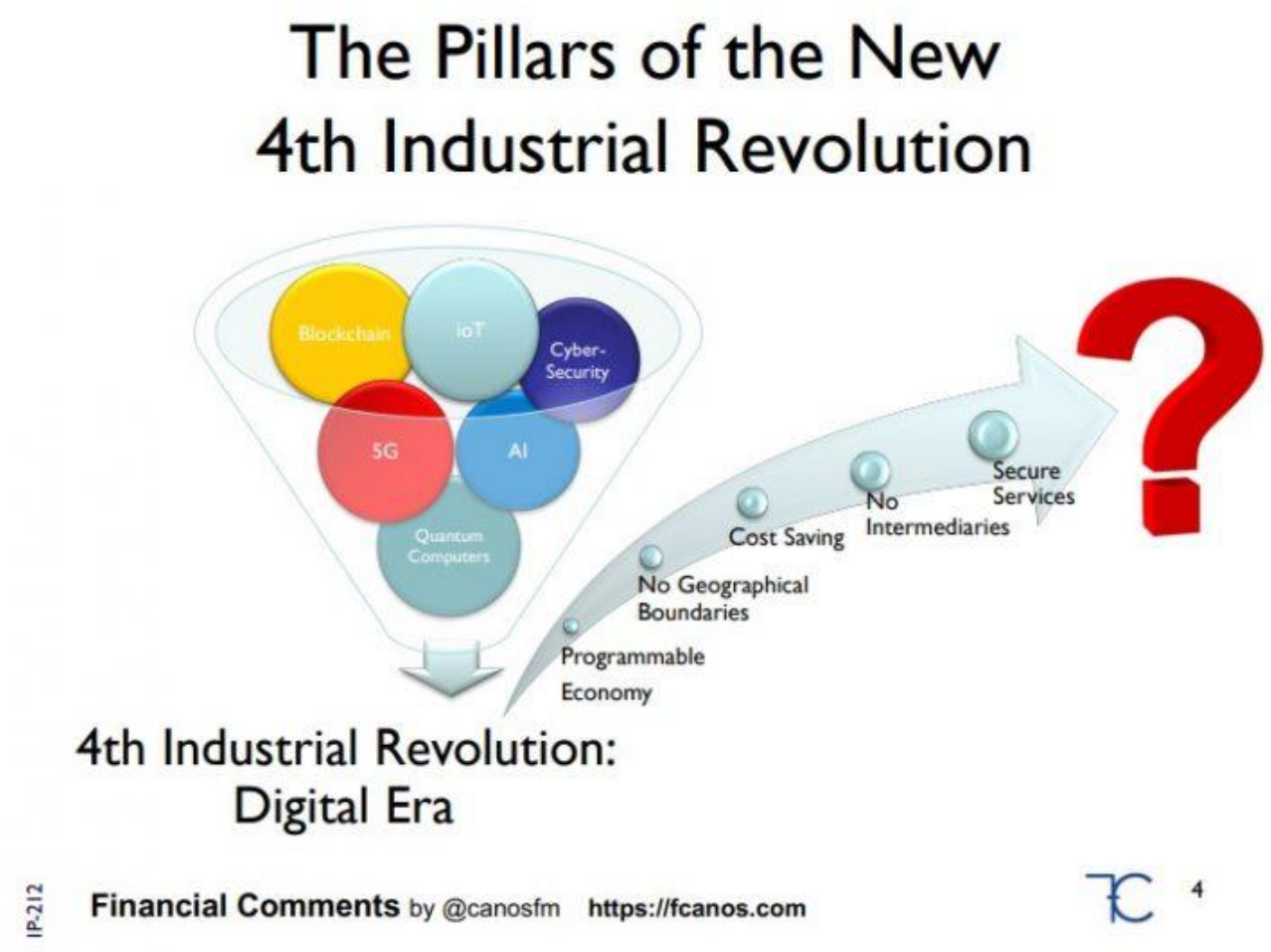
Tidak memahami inovasi *disruptive*

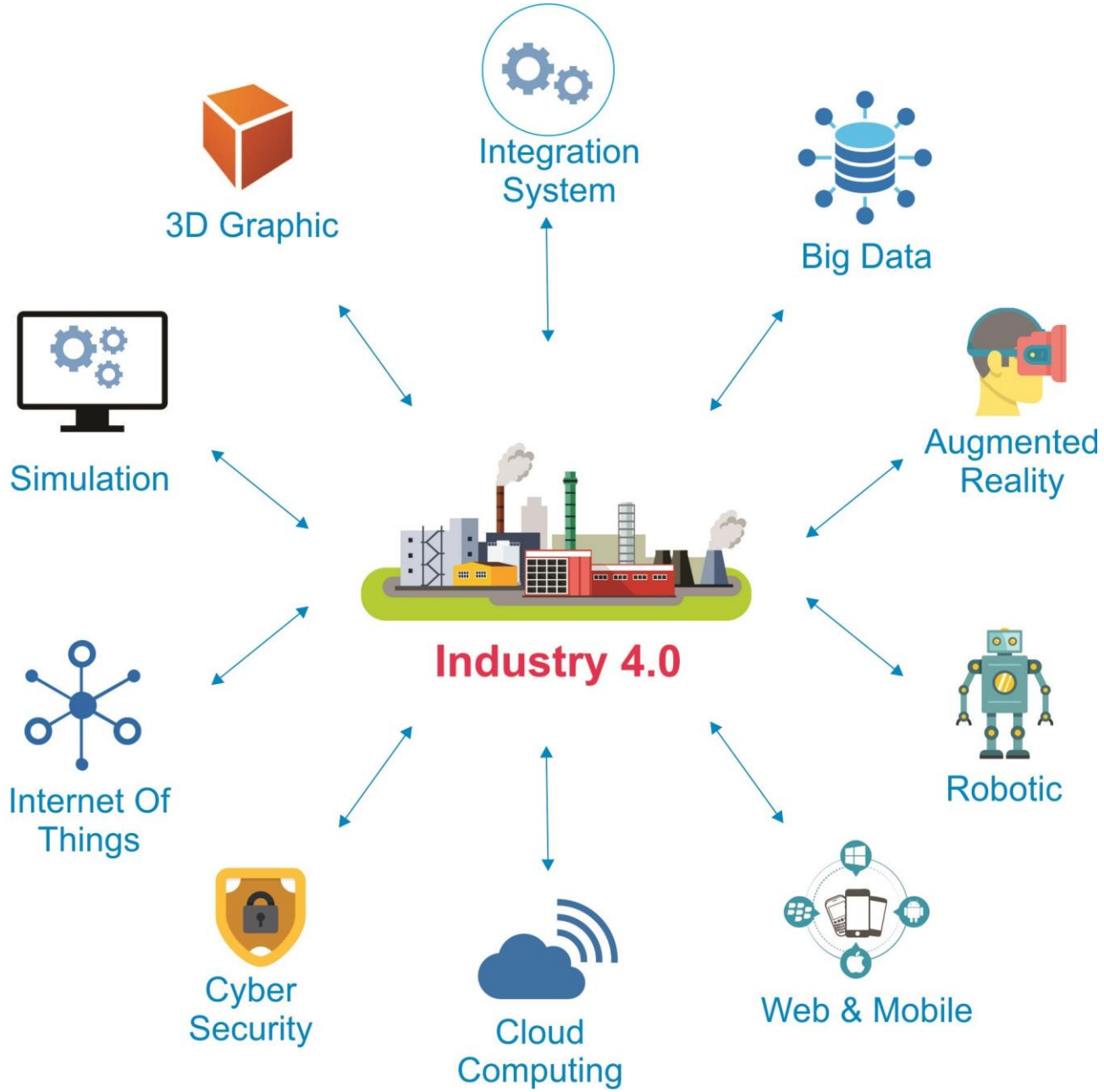
Beradaptasi dengan cepat dengan teknologi baru

Blockchain adalah inovasi teknologi dalam bidang ICT

- Blockchain dan AI (*Artificial Intelligence*) sering disebut pemimpin terdepan dalam revolusi industri 4.0.

- Menurut fcanos.com beberapa karakter revolusi industri ke 4 adalah tidak ada batas geografis, *cost saving*, tidak ada *intermediary*, *service* yang aman. Karakter ini semua ada pada teknologi blockchain.




Integration System
3D Graphic
Big Data
Simulation
Augmented Reality
Industry 4.0
Internet Of Things
Robotic
Cyber Security
Cloud Computing
Web & Mobile