

Bahan Kuliah IF4020 Kriptografi

Pengantar Blockchain

Oleh:

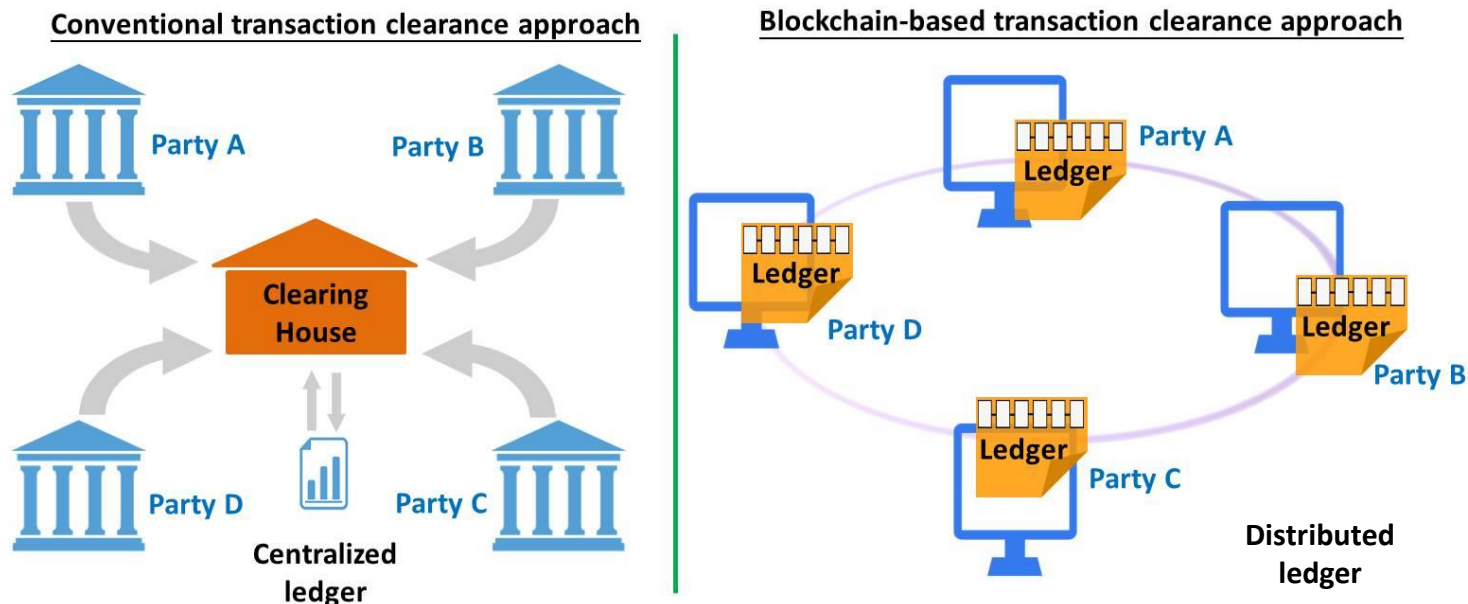
Dr. Ir. Rinaldi, M.T

**Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika (STEI)
ITB**



Blockchain

- **Blockchain** adalah sebuah *ledger* digital terdistribusi dan tidak mudah diubah yang merekam transaksi secara berurutan dalam “blok” yang saling terhubung secara kriptografis.
- Blockchain tidak mengenal pihak ketiga yang memiliki akses penuh terhadap keseluruhan data.
- Berbeda dengan pencatatan konvensional yang *centralized* dan membutuhkan pihak ketiga (misalnya bank)



Di dalam bidang akuntansi, *ledger* adalah buku besar yang mencatat semua transaksi keuangan dalam suatu periode tertentu

Kode : 11	Bulan : 11
Nama Akun : Kas	Tahun : 2010
Saldo Awal Debet: 0	Mutasi Debet: 9,800,000
Saldo Awal Kredit: 0	Mutasi Kredit: 7,980,000
Saldo Akhir Debet: 1,820,000	Saldo Akhir Kredit: 0

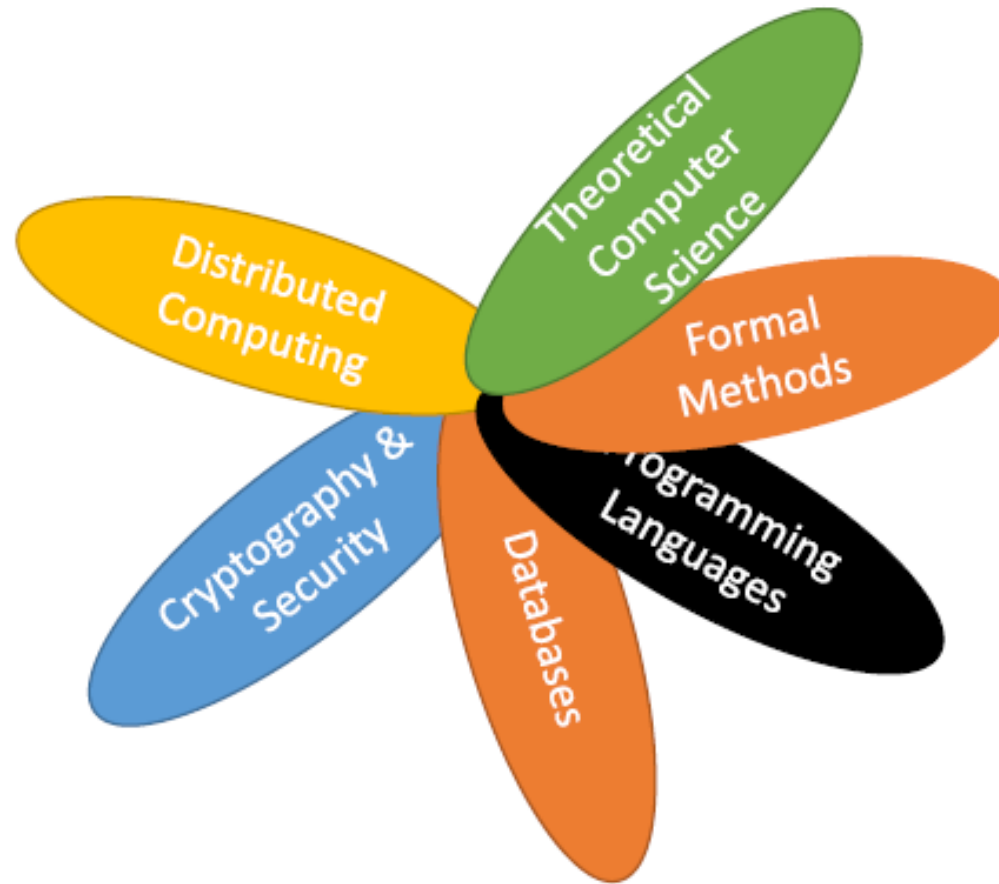
Tanggal	Keterangan	No Ref	Debet	Kredit	Saldo	
					Debet	Kredit
16-Nov-2010	Satoran Modal Awal	101101	4,000,000	0	4,000,000	0
17-Nov-2010	Meminjam uang ke Bank	101102	5,000,000	0	9,000,000	0
18-Nov-2010	Pembelian Kendaraan	101103	0	7,400,000	1,600,000	0
20-Nov-2010	Pembayaran hutang dagang	101105	0	30,000	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		

- Karakteristik teknologi *blockchain*:
 - menghilangkan kebutuhan pihak ketiga yang dipercayai sebagai penengah dalam suatu transaksi
 - melibatkan banyak pihak yang justru tidak mempercayai satu sama lain
 - setiap transaksi dapat dilacak riwayatnya (*traceability*) karena ada *timestamp*
 - aman, karena menggunakan kriptografi, sangat sulit bagi salah satu pihak untuk mengubah atau menghapus transaksi di dalam *ledger*.

- Karena tidak membutuhkan pihak ketiga dalam transaksi, maka *blockchain* sangat cocok digunakan pada beberapa aplikasi seperti:
 - layanan keuangan dan perbankan,
 - layanan publik (rumah sakit, transportasi, pemerintahan, dll)
 - layanan keamanan (*data security*)
 - sistem penilaian reputasi,
 - *Internet of Things (IoT)*.
- Untuk bisnis atau bidang yang membutuhkan keandalan dan kejujuran yang tinggi seperti pemerintahan dan keuangan, *blockchain* sangat cocok digunakan karena transaksi yang dicatat tidak dapat dimodifikasi oleh siapapun.
- *Cryptocurrency* (uang kripto) adalah contoh penggunaan teknologi *blockchain* yang sukses.



Blockchain adalah sebuah multidisiplin



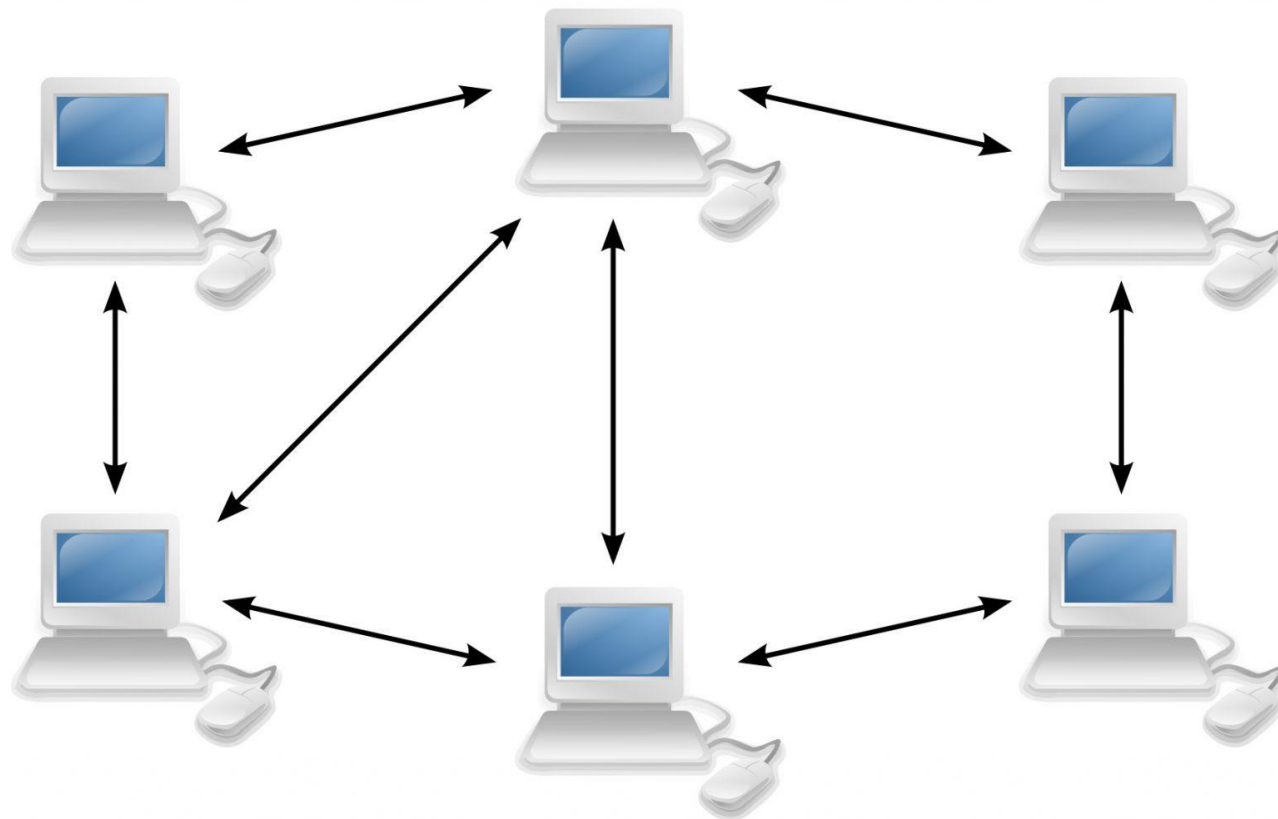
Penggunaan kriptografi di dalam *blockchain* (1)

1. **Hash kriptografis** (SHA-256, Keccak, dsb.) untuk integritas urutan blok.
2. **Tanda tangan digital** (ECDSA, Ed25519) untuk memastikan keaslian transaksi (siapa yang menandatangani).
3. **Merkle tree** untuk merangkum banyak transaksi di dalam satu root yang efisien verifikasinya.

Penggunaan kriptografi di dalam *blockchain* (2)

- Di dalam *blockchain*, setiap transaksi dicatat datanya di dalam *distributed ledger* menggunakan arsitektur *peer-to-peer*.
- Setiap data transaksi di dalam *ledger* direpresentasikan sebagai sebuah blok, dan blok-blok terhubung satu sama lain dalam suatu rantai secara kriptografis. Inilah asal mula kata *blockchain*.
- Setiap blok memiliki *pointer* ke blok sebelumnya. *Pointer* berisi nilai *hash* blok sebelumnya.
- Blok transaksi yang baru hanya dapat ditambahkan ke dalam *blockchain* dengan mekanisme konsensus antar *peer*.
- Blok yang sudah ditambahkan di dalam *blockchain* tidak dapat diubah atau dihapus lagi.
- Untuk memastikan keaslian transaksi, maka transaksi diberi tanda-tangan digital.
- Untuk menentukan apakah sebuah blok dapat diterima oleh semua *node*, maka digunakan mekanisme konsensus yang dinamakan *proof of work*.

- *Peer-to-peer* merupakan arsitektur jaringan yang digunakan oleh *blockchain* untuk menghubungkan lebih dari satu *node*, setiap *node* dapat berbagi dan mengakses sumberdaya secara langsung tanpa ada kontrol pusat atau *server* yang bertugas secara khusus. .

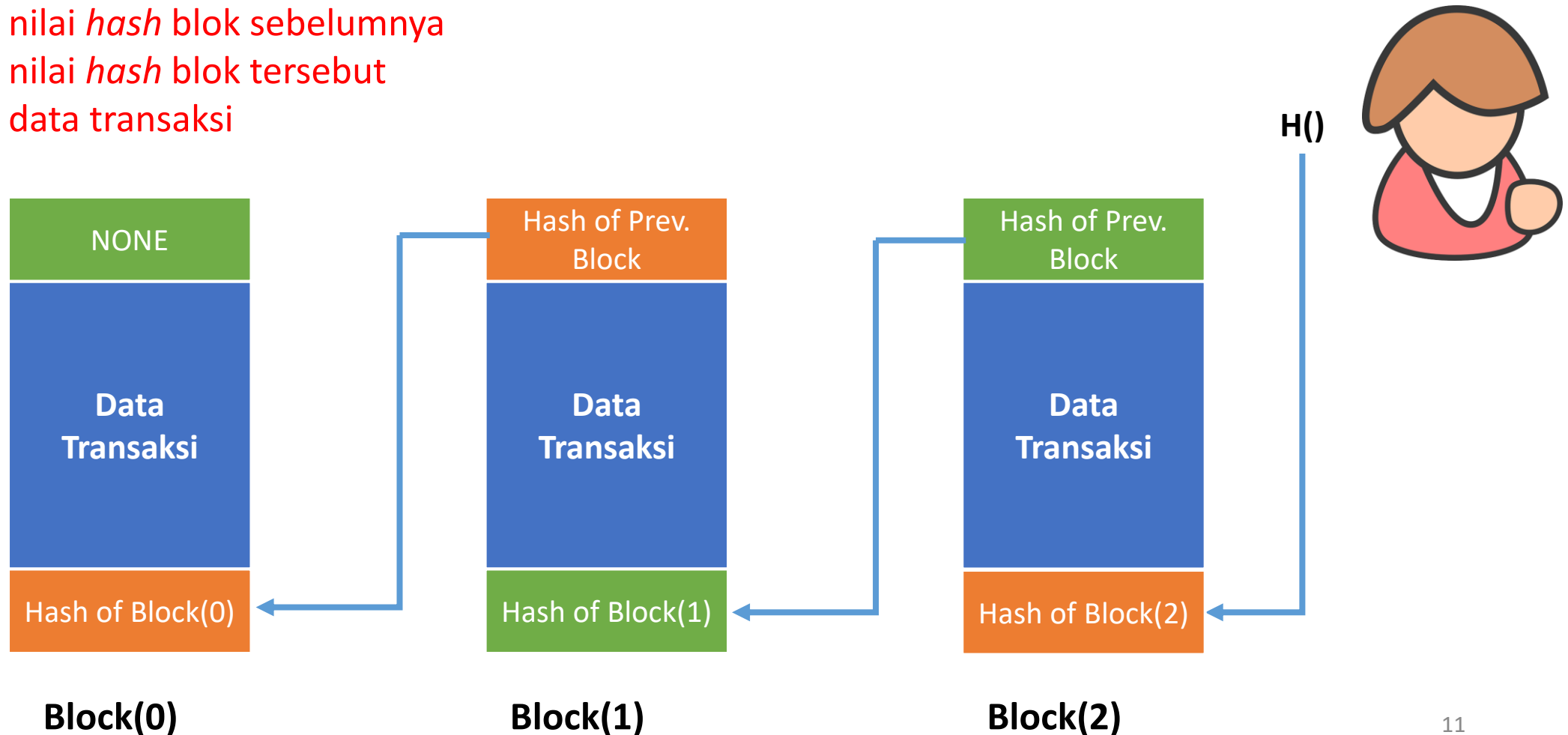


Blockchain

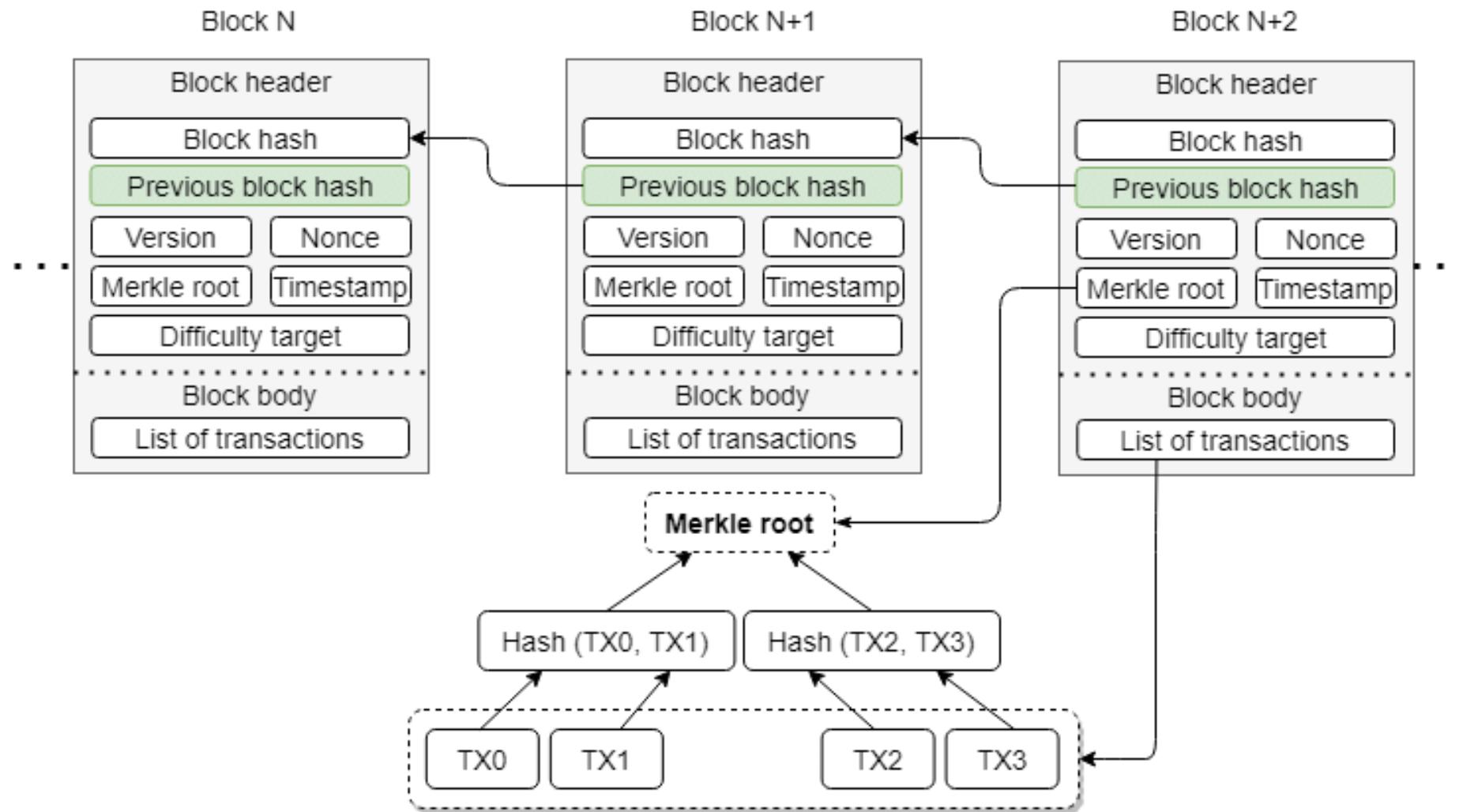
merangkai blok-blok data dengan menggunakan *hash pointer*

Setiap blok sedikitnya berisi informasi:

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



Komponen lebih rinci pada setiap blok:



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')
587b5ae6f25ebd8880fd86a7337d63622ae5661a0b9a13b7d21eee1d39613af
```

```
block_0
```

```
Out[85]:
```

```
{'prev_hash': None, 'time': 1575433243.9058905, 'data': 1,
 'current_hash': '05ad2692b90be260734b9fd151a4a471e6d2e06d616831f6efb1fc3e315c411f'}
```

```
block_1
```

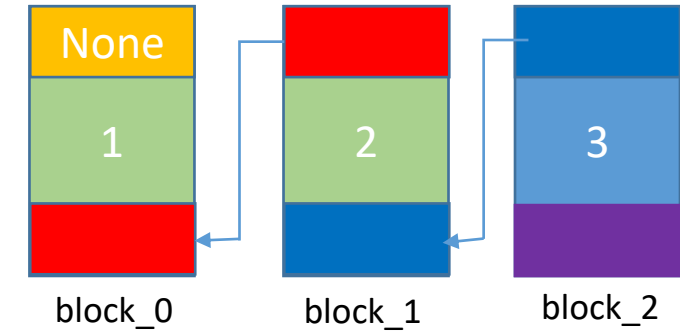
```
Out[86]:
```

```
{'prev_hash': '05ad2692b90be260734b9fd151a4a471e6d2e06d616831f6efb1fc3e315c411f',
 'time': 1575433243.9058905, 'data': 2,
 'current_hash': '4c6a3bb0730f6a3ff74b5a54b4f9706d7485ebf932d475440d619155093bac96'}
```

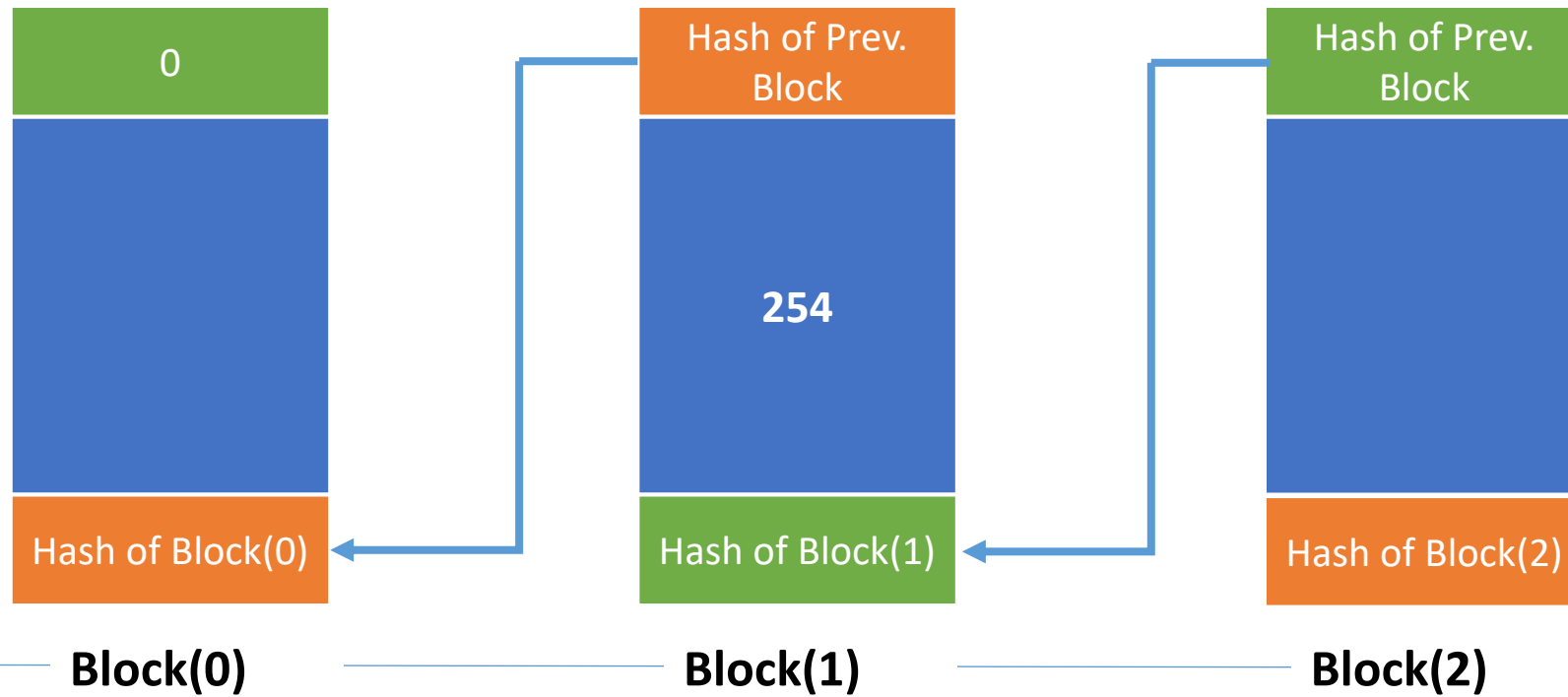
```
block_2
```

```
Out[87]:
```

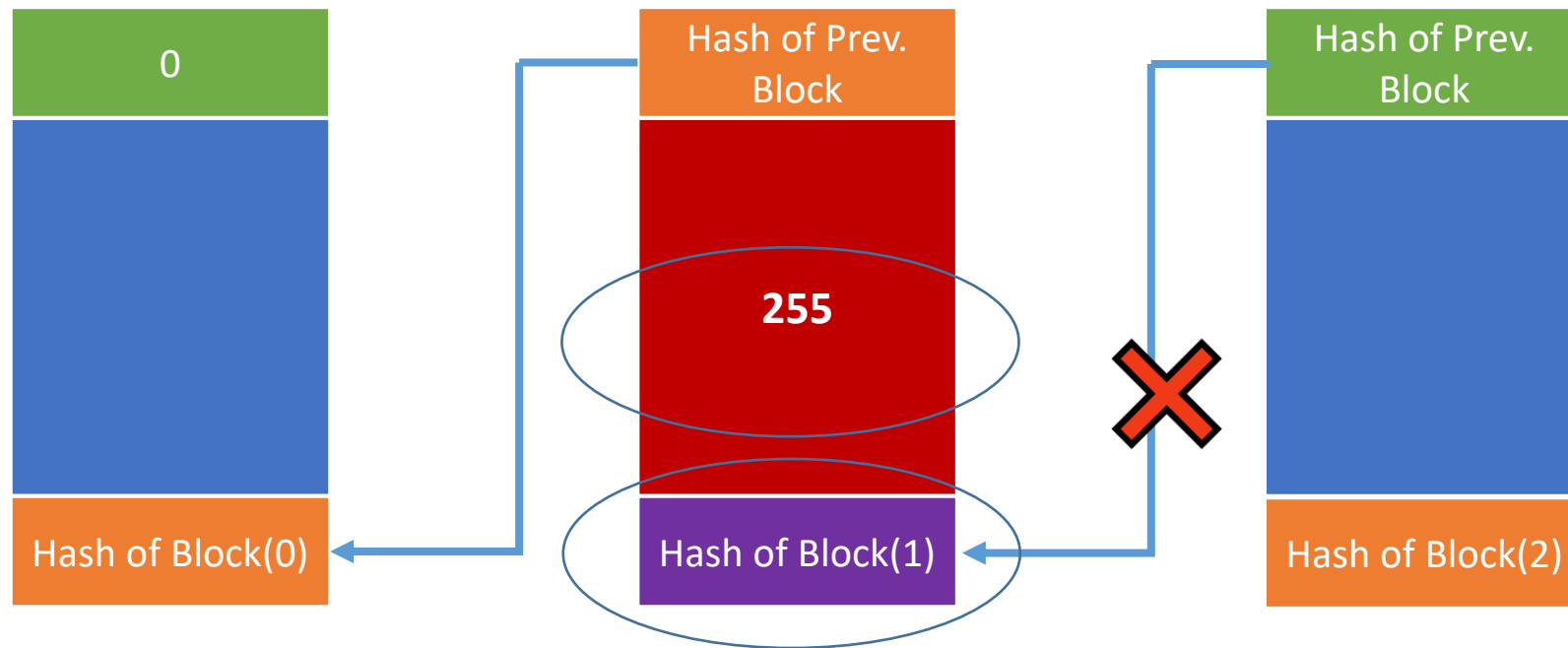
```
{'prev_hash': '4c6a3bb0730f6a3ff74b5a54b4f9706d7485ebf932d475440d619155093bac96',
 'time': 1575433243.9058905, 'data': 3,
 'current_hash': '587b5ae6f25ebd8880fd86a7337d63622ae5661a0b9a13b7d21eee1d39613af'}
```



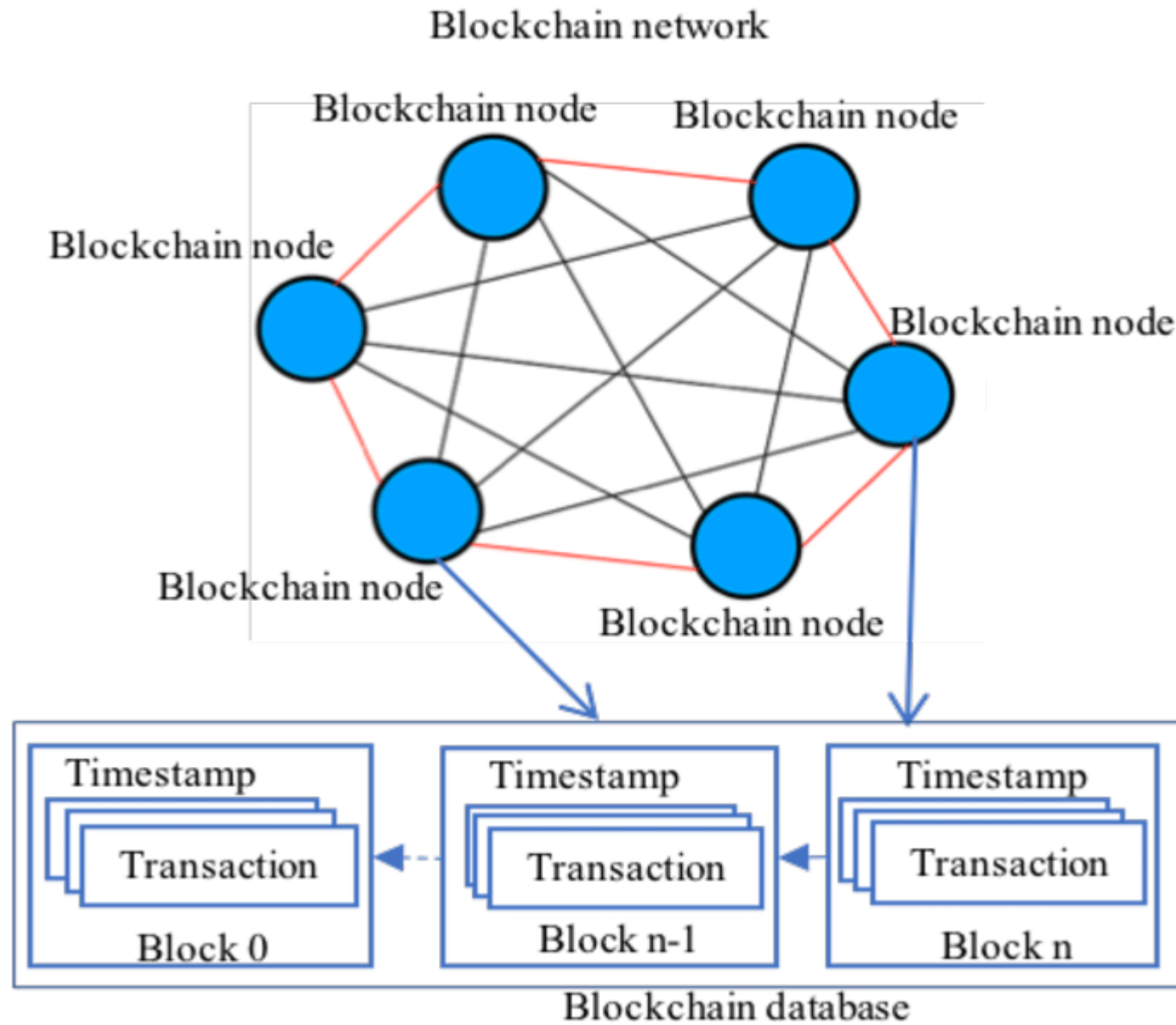
Data di dalam
blockchain
tidak dapat diubah



Seseorang
mengubah
data Block(1)



- Dengan adanya *block* yang harus memiliki nilai *hash block* sebelumnya, jika ada yang memaksa melakukan perubahan terhadap suatu *block* maka nilai *hash block* tersebut akan berubah dan keterhubungan antar *block* menjadi terputus.
- Karena *blockchain* bersifat terdistribusi, maka setiap *peer* pada jaringan *blockchain* tersebut akan memiliki catatan *record* yang sama sehingga jika ada satu *peer* yang melakukan perubahan maka *peer* yang lainnya akan melakukan pengecekan dan dapat dengan mudah menolak perubahan tersebut.
- Istilah jaringan pada *blockchain* merepresentasikan banyaknya *node* atau komputer yang saling terhubung satu sama lain. Setiap node akan memiliki semua catatan transaksi yang pernah tercatat dalam *blockchain*.



Langkah-langkah pembuatan blok di dalam blockchain

Kasus: keuangan

1. User Membuat Transaksi
 - User tanda tangan transaksi dengan private key
2. Transaksi disiarkan ke jaringan
3. Node menerima & memverifikasi transaksi
 - Valid signature?
 - Apakah saldo cukup? (untuk blockchain finansial)
 - Apakah *nonce* benar?
 - Apakah format transaksi valid?
4. Transaksi Masuk ke Mempool
 - Kumpulan transaksi menunggu untuk dimasukkan ke blok baru

5. Miners/Validators Mengusulkan Blok (Tergantung Konsensus)

- PoW : mencari nonce → harus memenuhi target hash.
- PoS : validator dipilih berdasarkan stake.
- BFT : voting antar node untuk menyetujui blok.

6. Blok ditemukan/diusulkan ke jaringan

- berisi: timestamp, daftar transaksi, hash-blok sebelumnya, dan data konsensus (nonce / signature validator)

7. Node memverifikasi blok baru

- Apakah hash blok valid?
- Apakah hash previous block cocok?
- Apakah transaksi di dalamnya valid semua?

8. Blok ditambahkan ke blockchain

- Menjadi bagian permanen dari chain → immutability

9. Jaringan mengupdate state

- Saldo/ledger diperbarui
- Status smart contract diperbarui

Demo *blockchain* pada *bitcoin*:

<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 independen 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.



NOKIA
Connecting People



Tidak memahami inovasi *disruptive*



Google

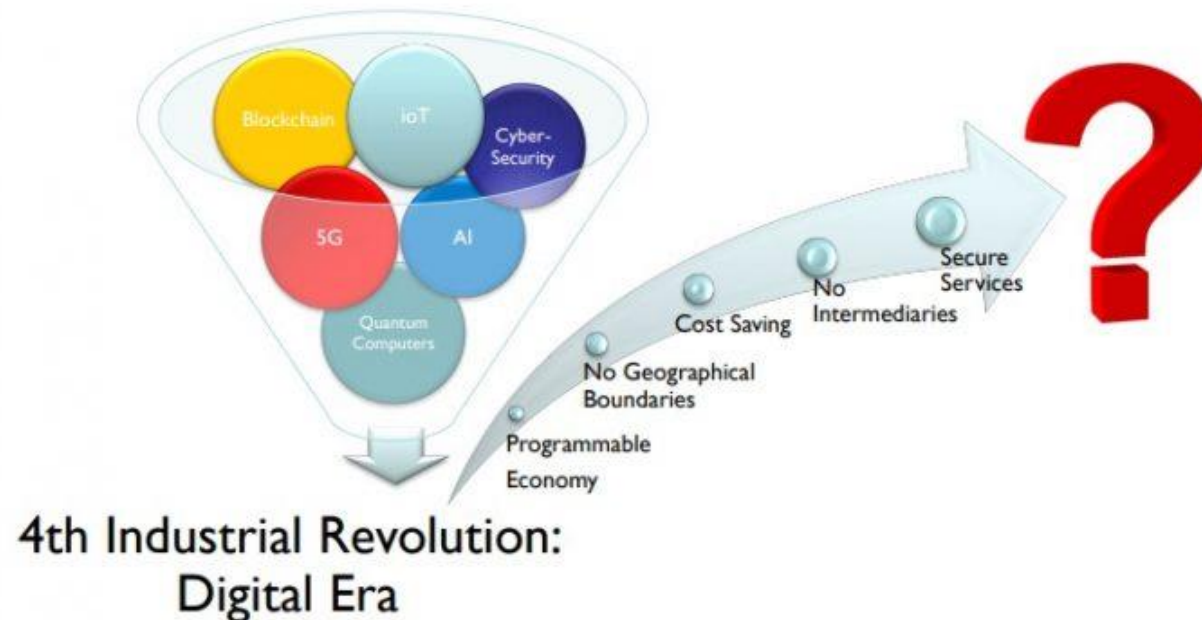


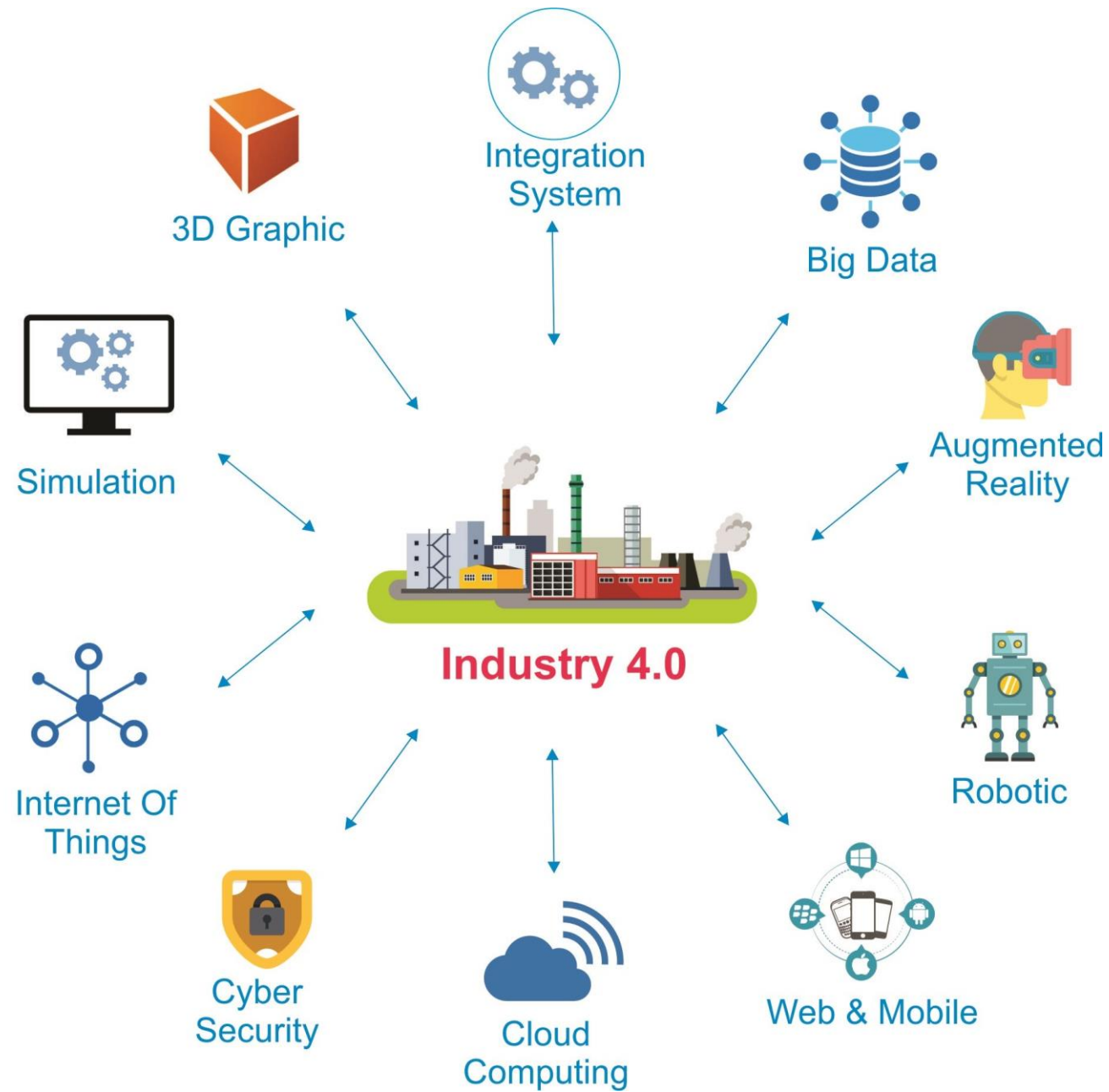
Beradaptasi dengan cepat dengan teknologi baru

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.

The Pillars of the New 4th Industrial Revolution





Klasifikasi Blockchain

Berdasarkan model perizinannya, *blockchain* dapat diklasifikasikan sebagai *public blockchain* dan *private blockchain*.

1. ***Public blockchain***

- semua orang dapat bergabung ke jaringan *blockchain* dan dapat menambahkan blok baru tanpa membutuhkan izin dari otoritas tertentu
- sering juga disebut juga dengan *permissionless blockchain*.
- setiap pengguna memiliki akses baca dan tulis ke *ledger*
- cocok untuk sistem yang membutuhkan anonimitas dari pihak lain di dalam jaringan blockchain. Ideal untuk transparansi & desentralisasi
- konsensus yang digunakan untuk menambahkan blok baru menggunakan sumber daya komputasi yang besar untuk mengantisipasi pihak ketiga yang berniat jahat
- Contoh public blockchain: *Bitcoin, ethereum*

2. *Private blockchain*

- hanya orang-orang yang telah terotorisasi oleh pihak berwenang di dalam jaringan yang dapat berpartisipasi di dalam jaringan *blockchain*
- sering juga disebut dengan *permissioned blockchain*.
- terdapat sebuah *node* yang memiliki otoritas untuk menyetujui seseorang bergabung ke dalam jaringan *blockchain*, mengontrol akses ke jaringan *blockchain*, dan mengatur akses baca dan tulis ke *ledger*
- biasanya digunakan oleh perusahaan yang perlu mengetahui identitas pihak-pihak yang terlibat di dalam transaksi.
- konsensus yang digunakan pada jaringan ini cenderung lebih sederhana dan tidak membutuhkan sumber daya komputasi berlebih karena jika terdapat pengguna yang bertindak jahat, pihak yang berwenang dapat mencabut hak aksesnya.

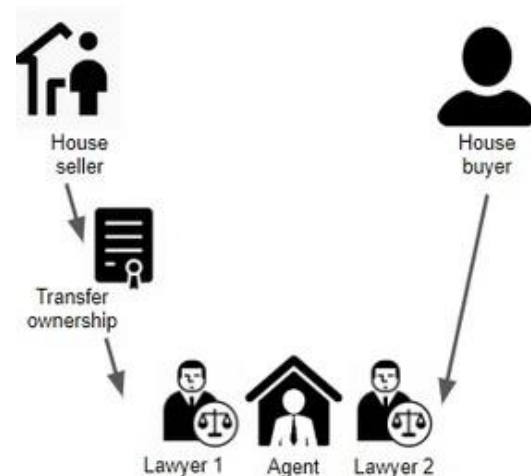
Metode Konsensus

- Untuk memutuskan apakah sebuah *peer* dapat menambahkan sebuah blok di dalam jaringan *blockchain*, maka diperlukan metode persetujuan untuk menyepakati *peer* mana yang dapat menambahkan blok.
- Metode persetujuan itu dinamakan *consensus*.
- Beberapa metode konsensus di dalam *blockchain*:
 1. *Proof of Work* (PoW) – menggunakan *puzzle*
 2. *Proof of Stake* (PoS) – menggunakan investasi sumberdaya
 3. *Round robin* (khusus untuk *permissioned blockchain*)
 4. *Proof of authority/identity*
 5. *Proof of Elapsed Time*

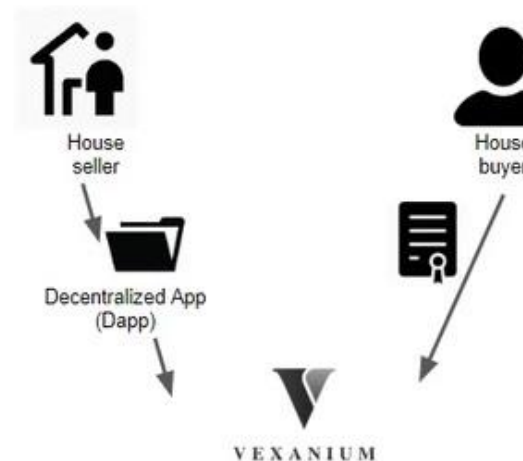
Smart Contract

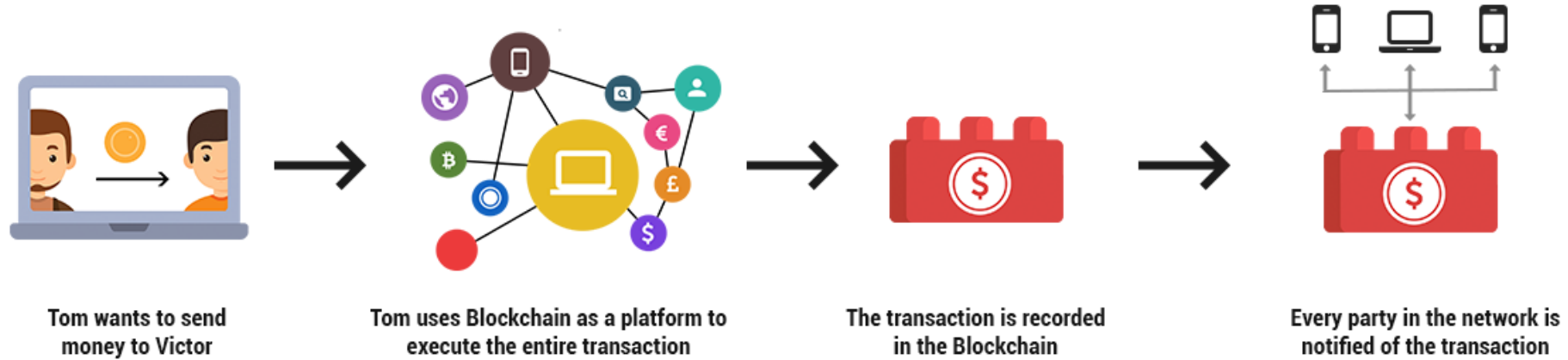
- *Smart contract* adalah protokol transaksi yang menjalankan beberapa syarat kontrak dengan menggunakan program komputer. Program *smart contract* berjalan di atas *blockchain*.
- Di dalam blockchain, *smart contract* digunakan untuk mengatur transaksi-transaksi, sehingga tidak memerlukan kuasa hukum.

TRADITIONAL CONTRACT

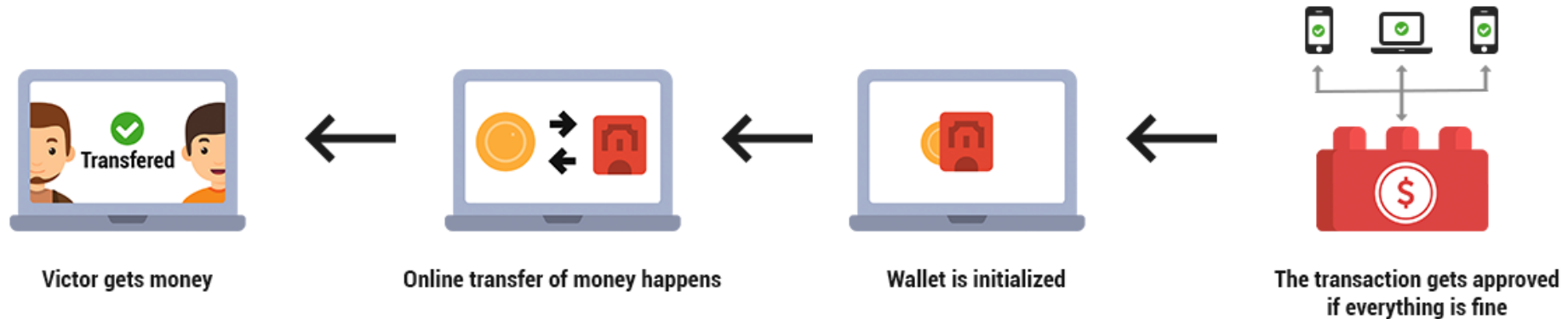


SMART CONTRACT





The entire task is completed using a Smart Contract



Hyperledger Fabric



- *Hyperledger Fabric* merupakan salah satu implementasi sistem blockchain.
- *Hyperledger Fabric* adalah platform teknologi *distributed ledger* yang dikembangkan oleh Linux Foundation. Platform ini merupakan proyek open source yang mengimplementasikan sistem blockchain bersifat *permissioned*.
- Hyperledger Fabric menjadi teknologi *blockchain* pertama yang memfasilitasi *smart contracts* yang dapat ditulis dengan Bahasa pemrograman umum seperti *Java, Go, Python, dan Javascript*.
- *Smart contracts* dalam *Hyperledger fabric* disebut sebagai *chaincode*

Sumber: Laporan TA M Zunan Alfikri

Pemrograman Blockchain dengan Python

- Baca: <https://www.geeksforgeeks.org/create-simple-blockchain-using-python/>