Bisa.ai
PT. Bisa Artifisial Indonesia

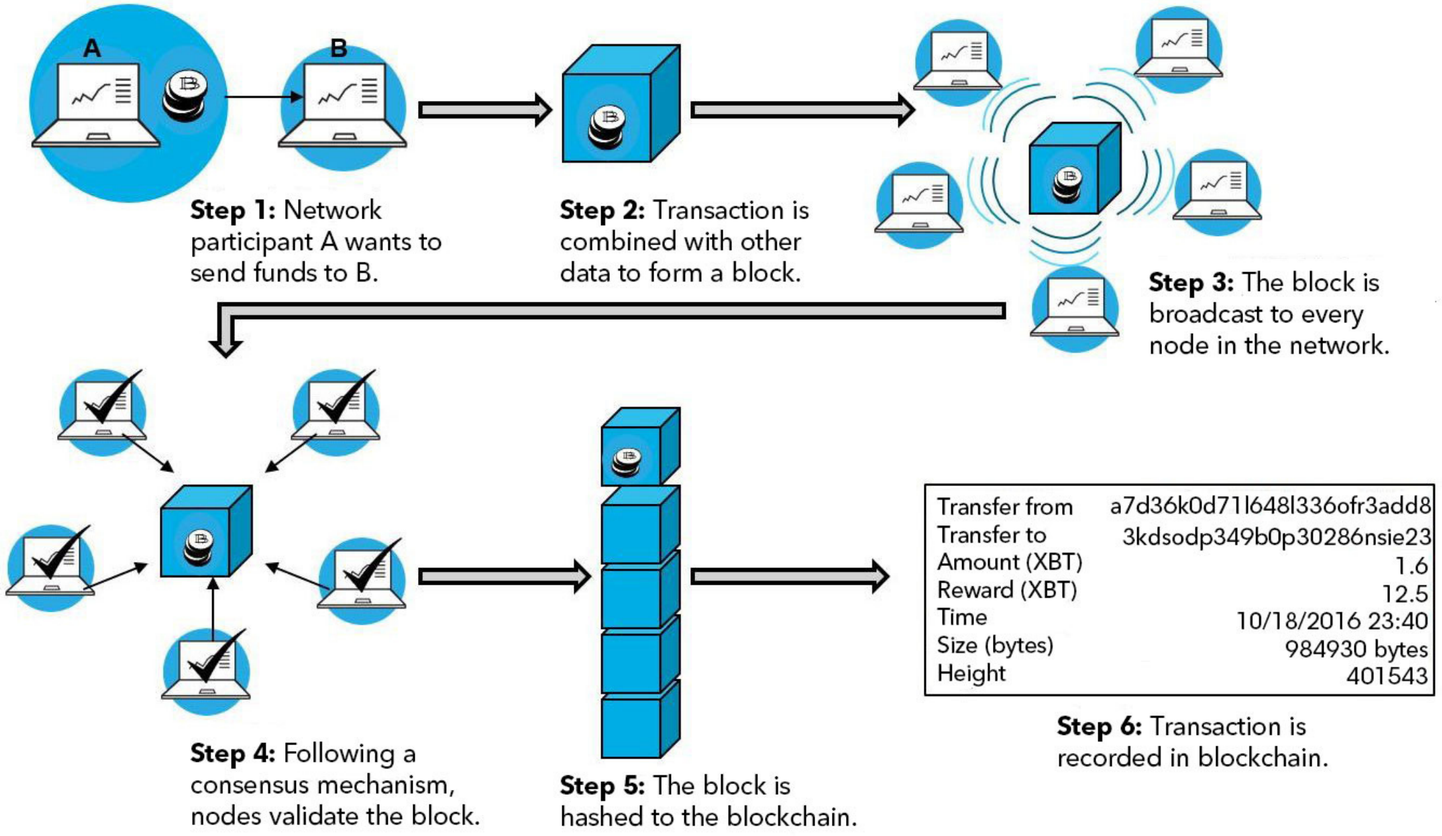
INTRODUCTION TO BLOCKCHAIN

M. Octaviano Pratama, S.Kom., M.Kom
Advisor Bisa AI Academy

BLOCKCHAIN

Blockchain

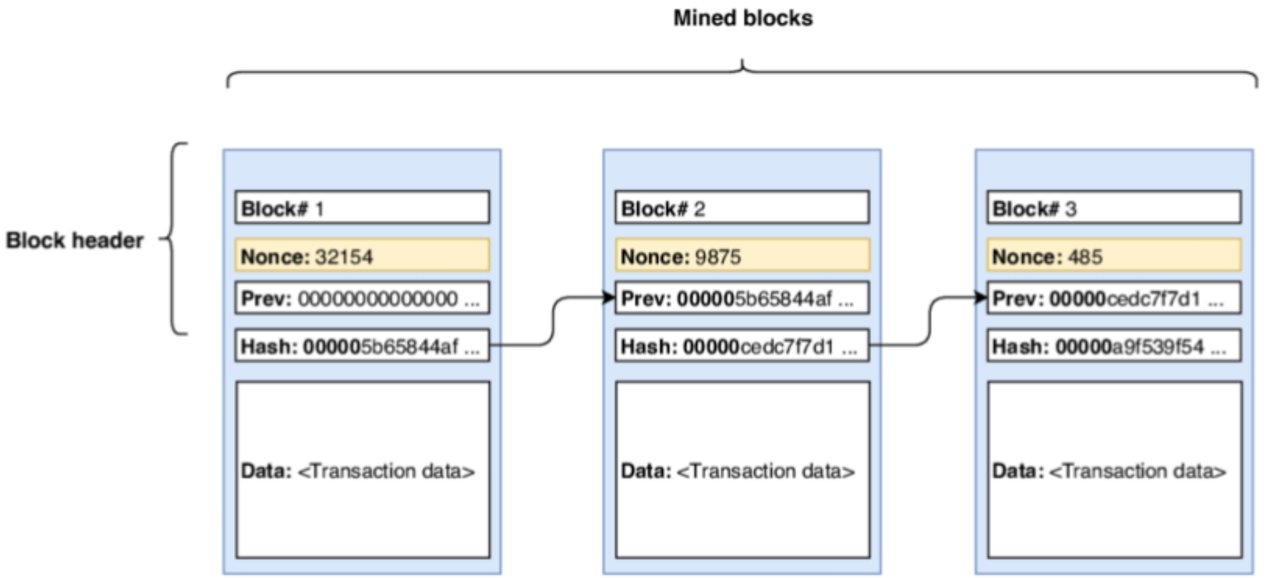
Technology that permits transactions to be gathered into blocks and recorded. allows the resulting ledger to be accessed by different servers. cryptographically chains blocks in chronological order; and



Source: Bloomberg NEF

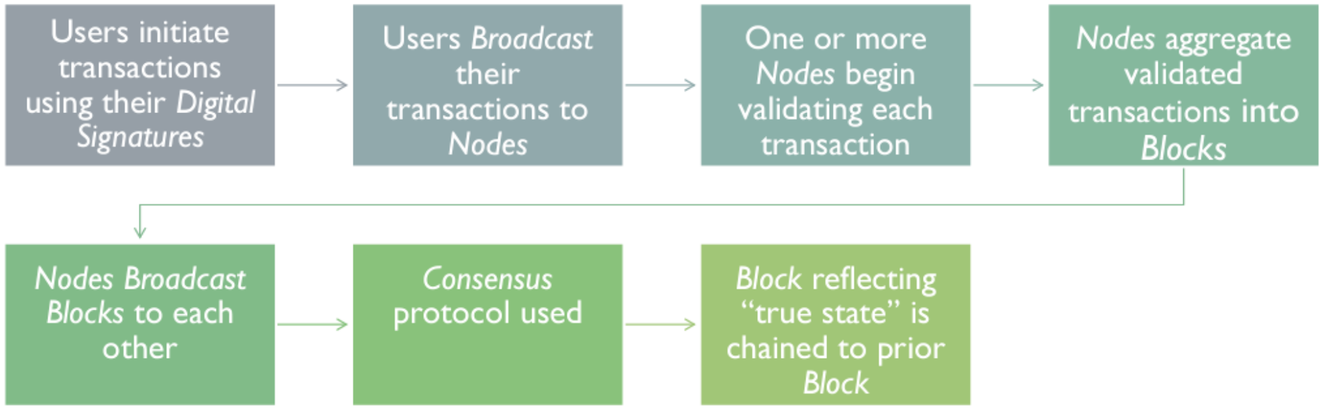
Blockchain

Teknologi Blockchain menjadi salah satu teknologi yang populer sejak kemunculan Bitcoin pada tahun 2009 melalui suatu publikasi dari kumpulan orang yang mengatasnamakan Satoshi Nakamoto. Ada banyak aplikasi dan kasus penggunaan yang dapat diselesaikan menggunakan blockchain selain hanya sistem pembayaran seperti sistem terdistribusi suatu jurnal dan sebagainya. Blockchain didefinisikan sebagai ledger terdistribusi peer to peer yang ditempa oleh consensus, dikombinasikan dengan sistem untuk smart contract



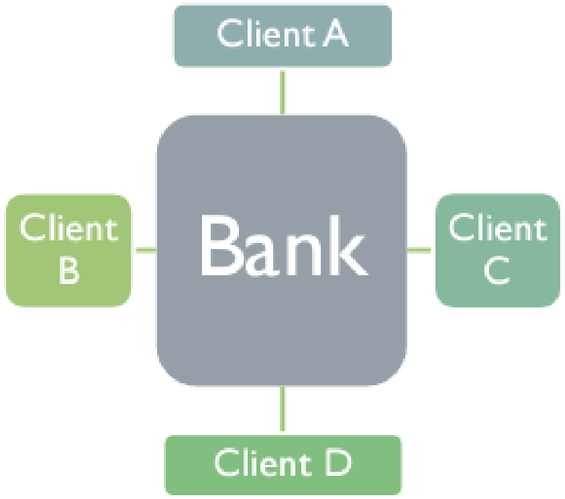
Distributed Ledger

Buku besar (ledger) adalah sistem yang berisi semua catatan input dan output dari suatu proses yang tersusun rapi di dalam buku besar. Distributed Ledger adalah struktur data yang tersebar di berbagai perangkat komputasi. DLT (Distributed Ledger Technology) adalah teknologi yang mendistribusikan catatan ke semua pengguna. Distributed Ledger Technology (DLT) mengacu pada infrastruktur teknologi dan protokol yang memungkinkan akses simultan, validasi, dan pembaruan catatan dengan cara yang tidak dapat diubah di seluruh jaringan yang tersebar di beberapa entitas atau lokasi. DLT terdiri dari 3 komponen: Model Data (keadaan buku besar saat ini), Bahasa transaksi (yang mengubah status buku besar) dan Protokol (digunakan untuk membangun konsensus). Blockchain adalah jenis DLT. DLT, lebih dikenal sebagai teknologi blockchain, diperkenalkan oleh Bitcoin dan sekarang menjadi kata kunci di dunia teknologi, mengingat potensinya di seluruh industri dan sektor. Dengan cara ini data dibagikan di antara semua penggunanya untuk meningkatkan transparansi dan menghindari korupsi.



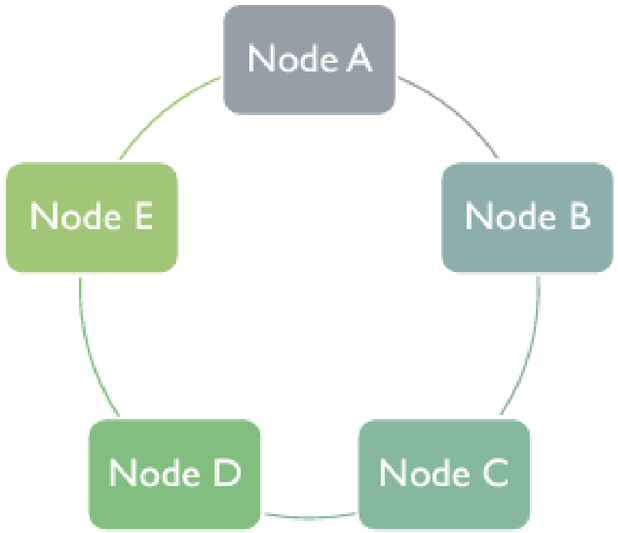
Distributed Ledger

Centralized Ledger



- There are multiple ledgers, but Bank holds the "golden record"
- Client B must reconcile its own ledger against that of Bank, and must convince Bank of the "true state" of the Bank ledger if discrepancies arise

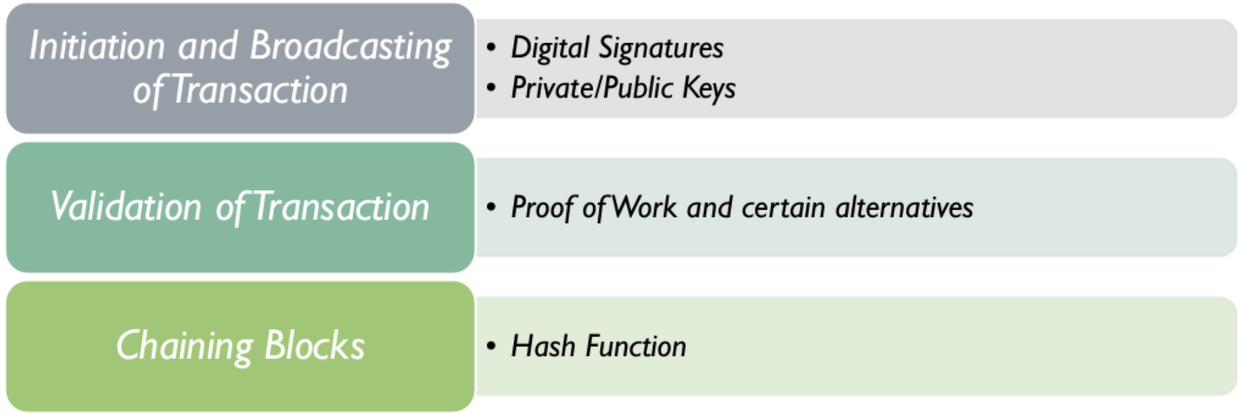
Distributed Ledger



- There is one ledger. All Nodes have some level of access to that ledger.
- All Nodes agree to a protocol that determines the "true state" of the ledger at any point in time. The application of this protocol is sometimes called "achieving consensus."

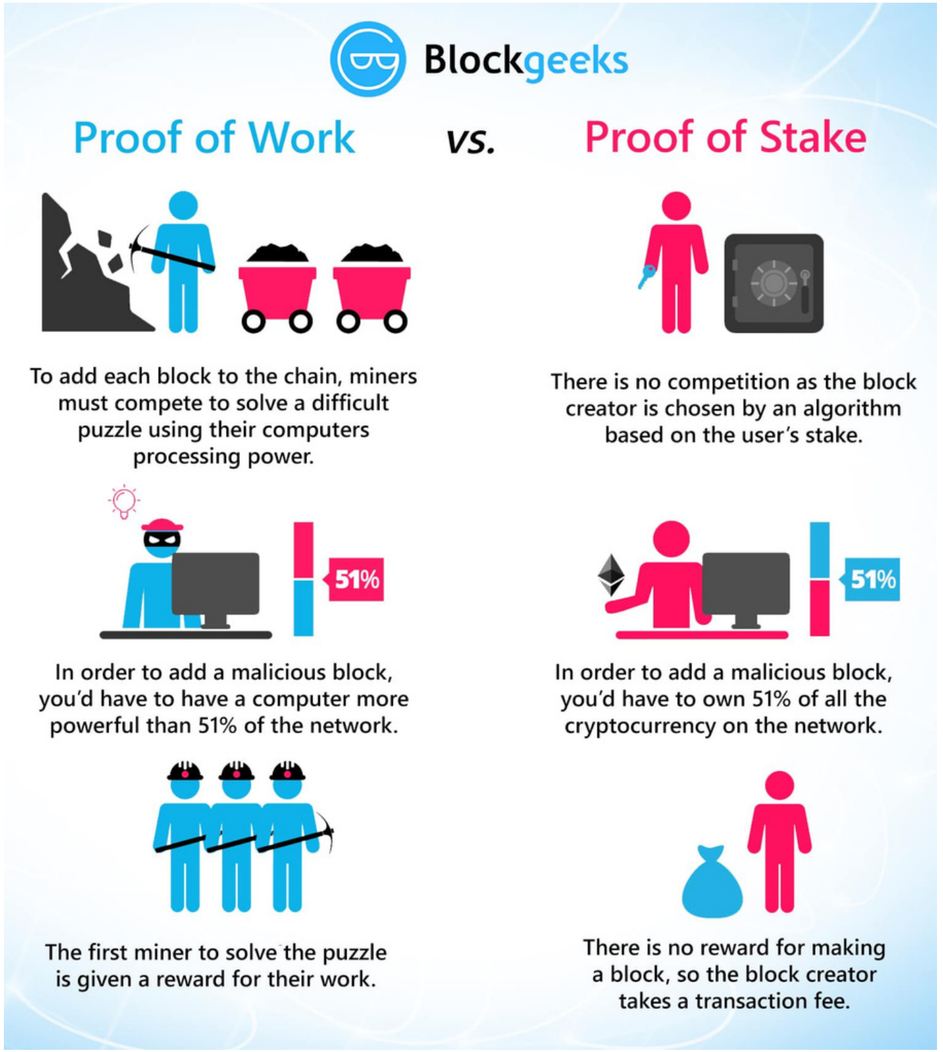
Kriptografi

Teknologi Blockchain berdasarkan konsep hubungan blok bersama menggunakan Kriptografi Hash. Fungsi Hash Kriptografi menerima setiap karakter input dan menciptakan output fixed-length yang merepresentasikan input. Nodes Blockchain menghitung nilai Hash pada blok dan menyimpan nilai pada blok lainnya pada chain. Setiap perubahan data, hash value akan berubah dan membuat link blok hash berikutnya tidak valid. Setiap perubahan akan membuat chain tidak valid.



Consensus

Konsensus adalah proses untuk memastikan bahwa semua pengguna yang berbeda dalam blockchain mencapai kesepakatan mengenai keadaan blockchain saat ini. Ada beberapa mekanisme konsensus yang digunakan oleh berbagai blockchain untuk mencapai konsensus. Misalnya, Bitcoin menggunakan Proof-of-Work sementara Ethereum berpindah dari algoritma Proof-of-Work ke Proof-of-Stake. Blockchain Node mengirimkan transaksi, kemudian special node disebut dengan miners mengumpulkan transaksi kedalam blok dan bersaing dengan miners lainnya untuk menjadi yang pertama menyelesaikan puzzle matematika yang membuat blok mudah untuk diverifikasi oleh node lainnya. Setiap blockchain dapat mendefinisikan metode yang berbeda untuk setiap node untuk memverifikasi blok, namun seluruh node di jaringan Blockchain menggunakan verifikasi blok yang sama. Metode yang digunakan Blockchain untuk memverifikasi validitas dari blok baru disebut algoritma consensus.



Blockchain Use Case in Finance

International Payments

For example, in April 2018, **Banco Santander launched the world's first blockchain-based money transfer service.** Known as "Santander One Pay FX," the service uses Ripple's xCurrent to enable customers to make same-day or next-day international money transfers. By automating the entire process on the blockchain, **Santander has reduced the number of intermediaries typically required in these transactions**, making the process more efficient. As a large commercial bank, Santander has numerous retail clients who would benefit from more efficient and cheaper payments, particularly in the area of international transfers. **Blockchain technology can be used to decrease the cost of these transfers by reducing the need for banks to manually settle transactions.**

Capital Market

Blockchain-based systems also have the potential to improve capital markets. Benefits: Faster clearing and settlement, Consolidated audit trail and Operational improvements. Startup Axoni was founded in 2013 and builds blockchain-based solutions specifically for capital market improvement. Most recently, Axoni announced the launch of a distributed ledger network to manage equity swap transactions – enabling both sides of an equity swap to be synchronized throughout their lifecycle, communicating changes to each other in real time.

Resources: https://www.insiderintelligence.com/insights/blockchain-technology-applications-use-cases/

Blockchain Use Case in Finance

Regulatory Compliance and Audit

The extremely secure nature of blockchain makes it rather useful for accounting and auditing because it significantly decreases the possibility of human error and ensures the integrity of the records. On top of this, no one can alter the account records once they are locked in using blockchain tech, not even the record owners. The trade off here is that blockchain tech could ultimately eliminate the need for auditors and erase jobs.

Money Laundering Protection

Once again, the encryption that is so integral to blockchain makes it exceedingly helpful in combating money laundering. The underlying technology empowers record keeping, which supports “Know Your Customer (KYC),” the process through which a business identifies and verifies the identities of its clients.

Insurance

Arguably the greatest blockchain application for insurance is through smart contracts. These contracts allow customers and insurers to manage claims in a transparent and secure manner. All contracts and claims can be recorded on the blockchain and validated by the network, which would eliminate invalid claims, since the blockchain would reject multiple claims on the same accident.

For example, openIDL, a network built on the IBM Blockchain Platform with the American Association of Insurance Services, is automating insurance regulatory reporting and streamlining compliance requirements.

Blockchain Use Case in Business

Supply Chain Management

Blockchain's immutable ledger makes it well suited to tasks such as real-time tracking of goods as they move and change hands throughout the supply chain. Using a blockchain opens up several options for companies transporting these goods. Entries on a blockchain can be used to queue up events with a supply chain — allocating goods newly arrived at a port to different shipping containers, for example. Blockchain provides a new and dynamic means of organizing tracking data and putting it to use.

Healthcare

Health data that's suitable for blockchain includes general information like age, gender, and potentially basic medical history data like immunization history or vital signs. On its own, none of this information would be able to specifically identify any particular patient, which is what allows it to be stored on a shared blockchain that could be accessed by numerous individuals without undue privacy concerns.

As specialized connected medical devices become more common and increasingly linked to a person's health record, blockchain can connect those devices with that record. Devices will be able to store the data generated on a healthcare blockchain and append it to personal medical records. A key issue currently facing connected medical devices is the siloing of the data they generate — but blockchain could be the link that bridges those silos.

Blockchain Use Case in Business

Real Estate

The average homeowner sells his or her home every five to seven years, and the average person will move nearly 12 times during their lifetime. With such frequent movement, blockchain could certainly be of use in the real estate market. It would expedite home sales by quickly verifying finances, reduce fraud thanks to its encryption, and offer transparency throughout the entire selling and purchasing process.

Energy

Blockchain technology could be used to execute energy supply transactions, but also to further provide the basis for metering, billing, and clearing processes, according to PWC. Other potential applications include documenting ownership, asset management, origin guarantees, emission allowances, and renewable energy certificates.

Blockchain Use Case in Government

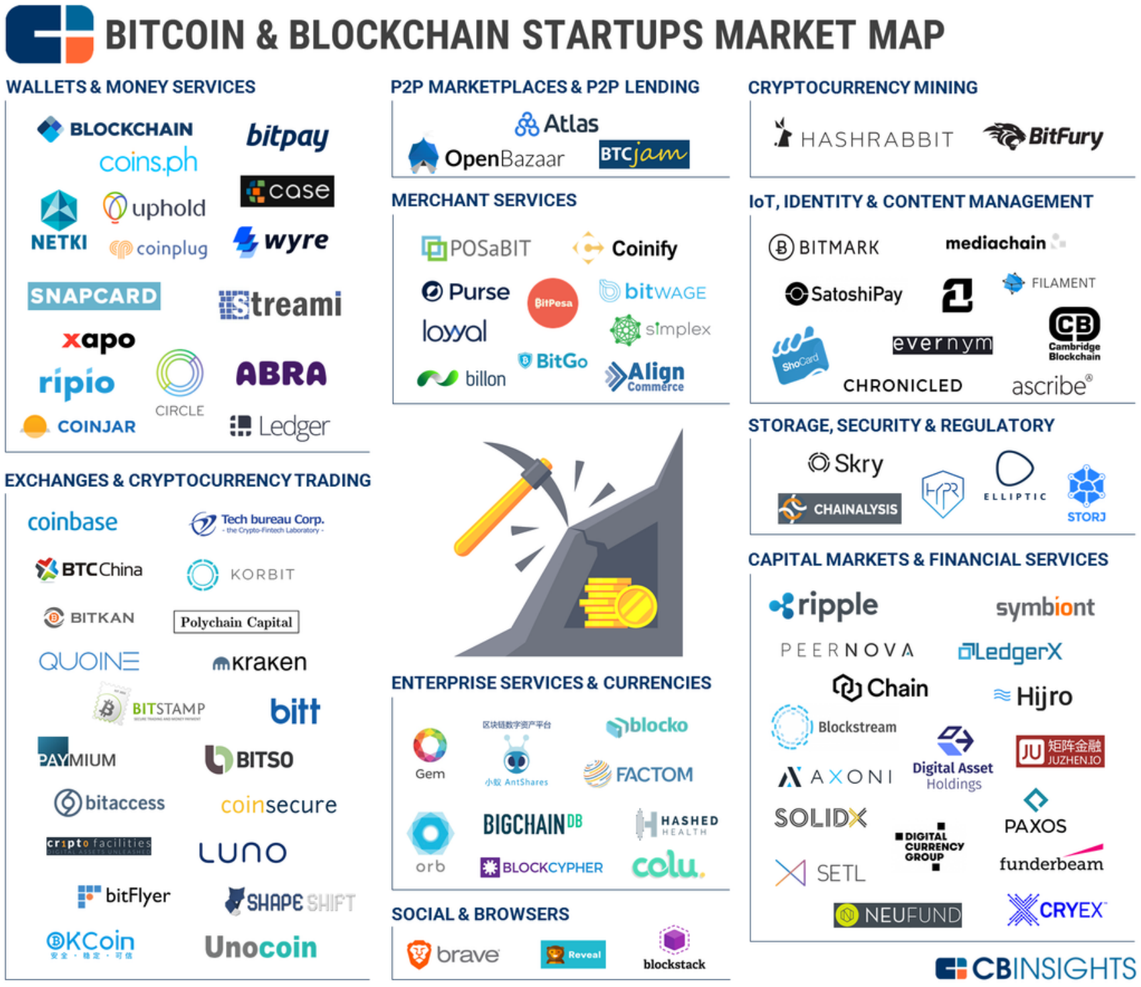
Record Management

National, state, and local governments are responsible for maintaining individuals' records such as birth and death dates, marital status, or property transfers. Yet managing this data can be difficult, and to this day some of these records only exist in paper form. And sometimes, citizens have to physically go to their local government offices to make changes, which is time-consuming, unnecessary, and frustrating. Blockchain technology could simplify this recordkeeping and make the data far more secure.

Voting

Blockchain technology has the ability to make the voting process more easily accessible while improving security. Hackers would be no match to blockchain technology, because even if someone were to access the terminal, they wouldn't be able to affect other nodes. Each vote would be attributed to one ID, and with the ability to create a fake ID being impossible, government officials could tally votes more efficiently and effectively.

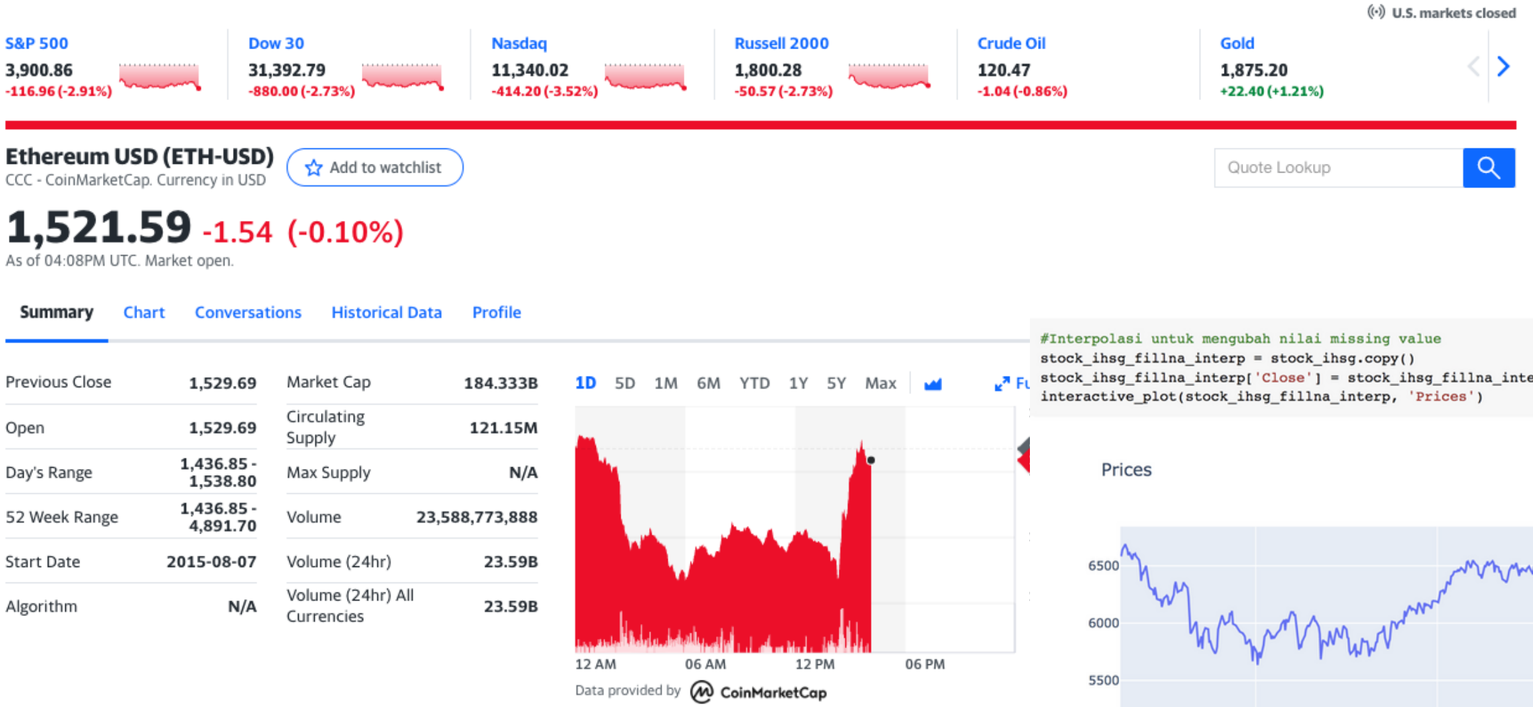
Blockchain Startup



Pada kuartal pertama tahun 2021 saja, perusahaan rintisan blockchain di seluruh dunia mengumpulkan **2,6 miliar dolar AS atau 37 Triliun** dalam pendanaan modal ventura.

PELUANG MAHASISWA INDONESIA SAAT INI ADALAH MEMBUAT DIGITAL STARTUP!

Get Cryptocurrency




```
#Interpolasi untuk mengubah nilai missing value
stock_ihsg_fillna_interp = stock_ihsg.copy()
stock_ihsg_fillna_interp['Close'] = stock_ihsg_fillna_interp['Close'].interpolate(method='linear')
interactive_plot(stock_ihsg_fillna_interp, 'Prices')
```

Blockchain Data Analytics

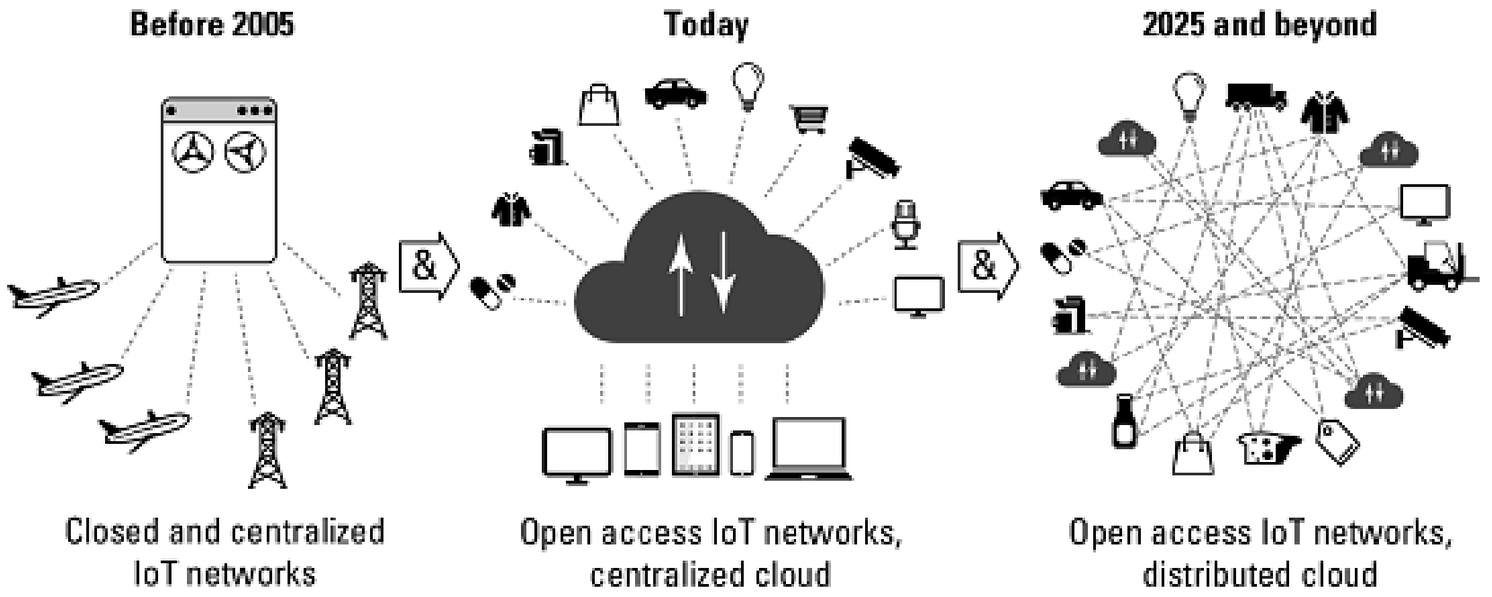
Accessing Public Financial Transaction Data

Audit data yang dihasilkan dari transaksi Blockchain dapat dilakukan dengan teknik data analytics

Date	Open	High	Low	Close*	Adj Close**	Volume
Jun 12, 2022	1,529.69	1,538.80	1,436.85	1,525.35	1,525.35	23,571,193,856
Jun 11, 2022	1,665.22	1,679.31	1,507.04	1,529.66	1,529.66	21,127,089,064
Jun 10, 2022	1,789.69	1,797.61	1,663.43	1,665.04	1,665.04	18,504,740,451
Jun 09, 2022	1,793.51	1,827.29	1,779.87	1,789.83	1,789.83	12,013,083,393
Jun 08, 2022	1,814.10	1,830.68	1,770.23	1,793.57	1,793.57	18,041,476,023
Jun 07, 2022	1,859.33	1,862.91	1,729.41	1,814.05	1,814.05	24,020,076,750
Jun 06, 2022	1,805.64	1,915.03	1,804.99	1,859.29	1,859.29	16,518,471,852
Jun 05, 2022	1,801.82	1,825.86	1,777.13	1,805.20	1,805.20	8,850,385,937
Jun 04, 2022	1,775.22	1,810.30	1,751.53	1,801.61	1,801.61	8,677,951,273

Blockchain Data Analytics

Analysis of IoT Data



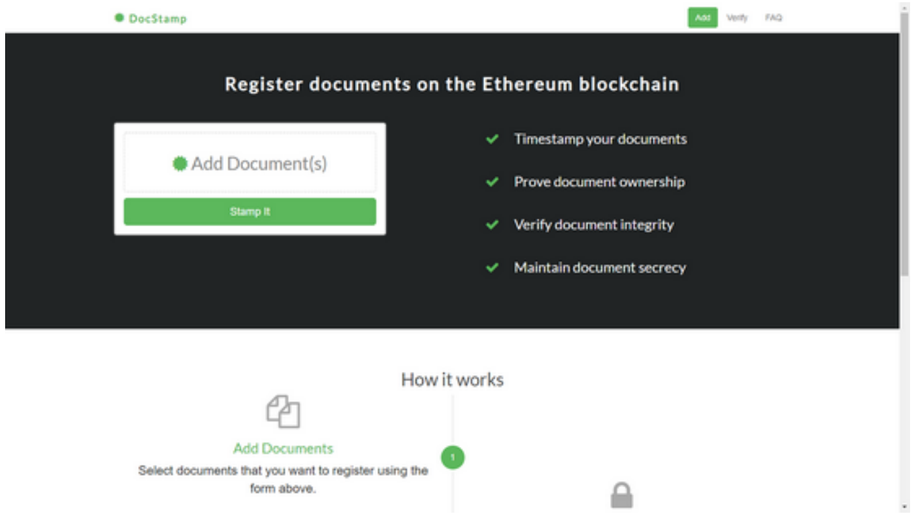
Many companies working in the IoT are looking to leverage the smart contracts in blockchain networks to allow IoT devices to work more securely and autonomously

Blockchain Data Analytics

Ensuring Data and Document Authentic

In the era of deep fakes, manipulated photos and consistently evolving methods of corruption and misappropriation of funds, blockchain can help identify cases of data fraud and misuse. Blockchain's inherent transparency and immutability means that data cannot be retroactively manipulated to support a narrative. Facts in a blockchain are recorded as unchangeable facts. Analytics models can help researchers understand how data of any type originated, who the original owner was, how it gets amended over time, and if any amendments are coordinated.

Controlling secure document integrity



The company DocStamp has implemented a novel use for blockchain document management. Using DocStamp, shown below, anyone can self-notarize any document. The document owner maintains control of the document while storing a hash of the document on an Ethereum blockchain.

Blockchain Data Analytics

Tracking Supply Chain

Blockchain-based supply chain solutions are one of the most popular ways to implement blockchain technology. Blockchain technology makes it easy to track items along the supply chain, both forward and backward. The capability to track an item makes it easy to determine where an item is and where that item has been. Tracing an item's provenance, or origin, makes root cause analysis possible. Because the blockchain keeps all history of movement through the supply chain, many types of analysis are easier than traditional data stores which can overwrite data.

Empowering predictive analytics

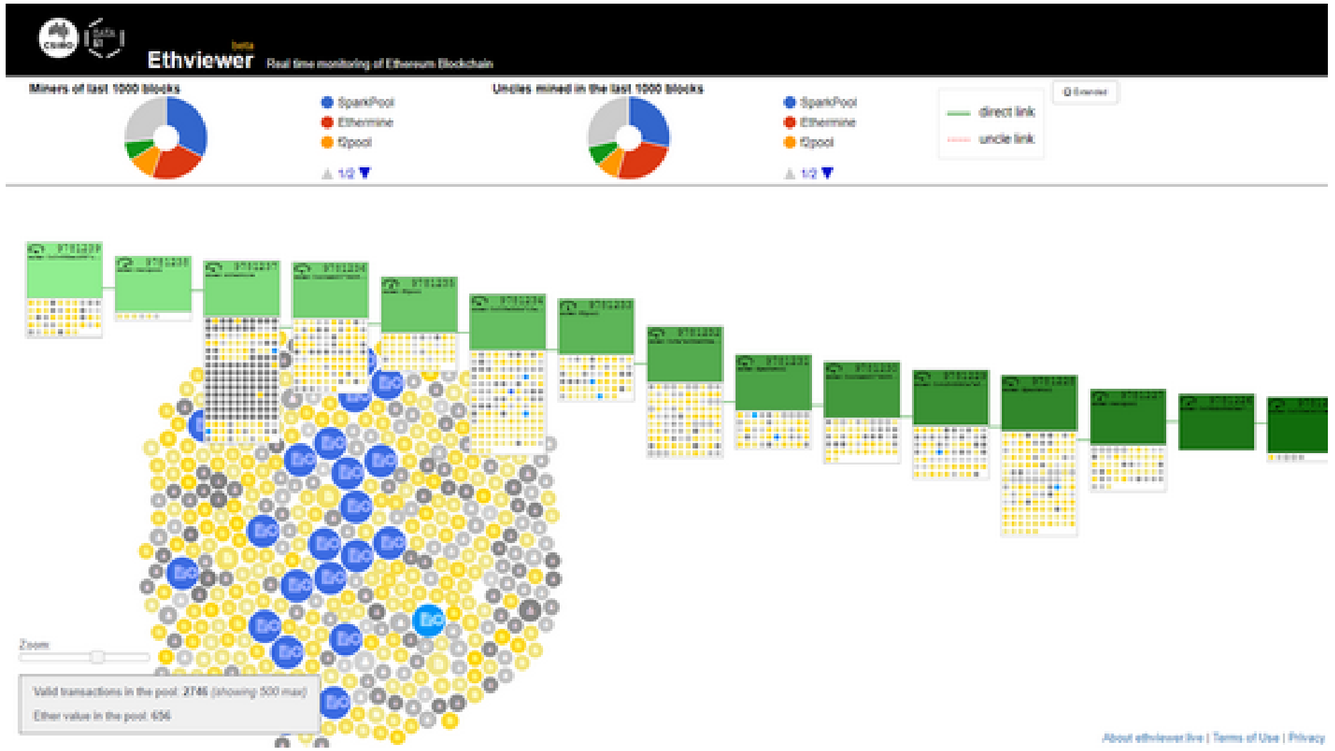
In the past, a common approach to acquiring enough data for meaningful analysis was to purchase data from an aggregator. Each data acquisition request costs money, and the data you receive may still be limited in scope. The prospect of using public blockchains has the potential to change the way we all access public data. If a majority of supply chain interactions, for example, use a public blockchain, that data is available to anyone — for free.
As more organizations incorporate blockchains into their operations, analysts could leverage the additional data to empower more companies to use predictive analytics with less reliance on localized data.

Blockchain Data Analytics

Analysis Real-time Data

Blockchain transactions happen in real time, across intranational and international borders. Not only are banks and innovators in financial technology pursuing blockchain for the speed it offers to transactions, but data scientists and analysts are observing blockchain data changes and additions in real time, greatly increasing the potential for fast decision-making.

To view how dynamic blockchain data really is, visit the Ethviewer Ethereum blockchain monitor's website. The following image shows the Ethviewer website.



Case Study Lainnya

- Analisa Perpindahan Ternak pada e-livestock
- Analisa komoditas bidang pertanian
- Analisa penjualan kendaraan

PROGRAMMING

Blockchain Programming

Blockchain

```
import hashlib
import json

class Block:
 hash = None
 data = None
 prev_hash = None

A = Block()
A.prev_hash = None
A. hash = hashlib.sha256(json.dumps(A.__dict__)
 .encode('utf-8')).hexdigest()
A.data = "Transaksi Rp. 50.000 dari A ke B"

B = Block()
B.prev_hash = A.hash
B. hash = hashlib.sha256(json.dumps(B.__dict__)
 .encode('utf-8')).hexdigest()
B.data = "Transaksi Rp. 10.000 dari B ke C"

C = Block()
C.prev_hash = B.hash
C. hash = hashlib.sha256(json.dumps(C.__dict__)
 .encode('utf-8')).hexdigest()
C.data = "Transaksi Rp. 5.000 dari C ke A"
```

Proof of Work

```
import hashlib
payload = b'{"prev_hash": "[hash sebelumnya]", "data": "Transaksi Rp. 500
dari D ke A"}'
for i in range(10000000):
 nonce = str(i).encode('utf-8')
 result = hashlib.sha256(payload + nonce).hexdigest()
 if result[0:5] == '00000':
   print(i)
   print(result)
   break

#Hasil:
#1930054 (nonce)
#000002c663021388331c7cd8d60bab8c99eae80a5991b52d07b6a1611a378a2e (hash)
```

Blockchain Programming

Cryptography

```
from cryptography.hazmat.primitives import hashes
from cryptography.hazmat.primitives.asymmetric import padding
from cryptography.hazmat.backends import default_backend
from cryptography.hazmat.primitives.asymmetric import rsa
from cryptography.hazmat.primitives import serialization

from google.colab import drive
drive.mount('/content/drive')

private_key_file = "/content/drive/My Drive/blockchain/octavkey.pem"
public_key_file = "/content/drive/My Drive/blockchain/octavkey.pub"
pesan = b"Octav bermain bola"

with open(private_key_file, "rb") as key_file:
 private_key = serialization.load_pem_private_key(
     key_file.read(),
     password=None,
     backend=default_backend()
 )

signature = private_key.sign(pesan,
   padding.PSS(
       mgf=padding.MGF1(hashes.SHA256()),
       salt_length=padding.PSS.MAX_LENGTH
   ),
   hashes.SHA256()
)
```

```
with open(public_key_file, "rb") as key_file:
 public_key = serialization.load_pem_public_key(
     key_file.read(),
     backend=default_backend()
 )

public_key.verify(
   signature,
   pesan,
   padding.PSS(
       mgf=padding.MGF1(hashes.SHA256()),
       salt_length=padding.PSS.MAX_LENGTH
   ),
   hashes.SHA256()
)

print(signature)
```

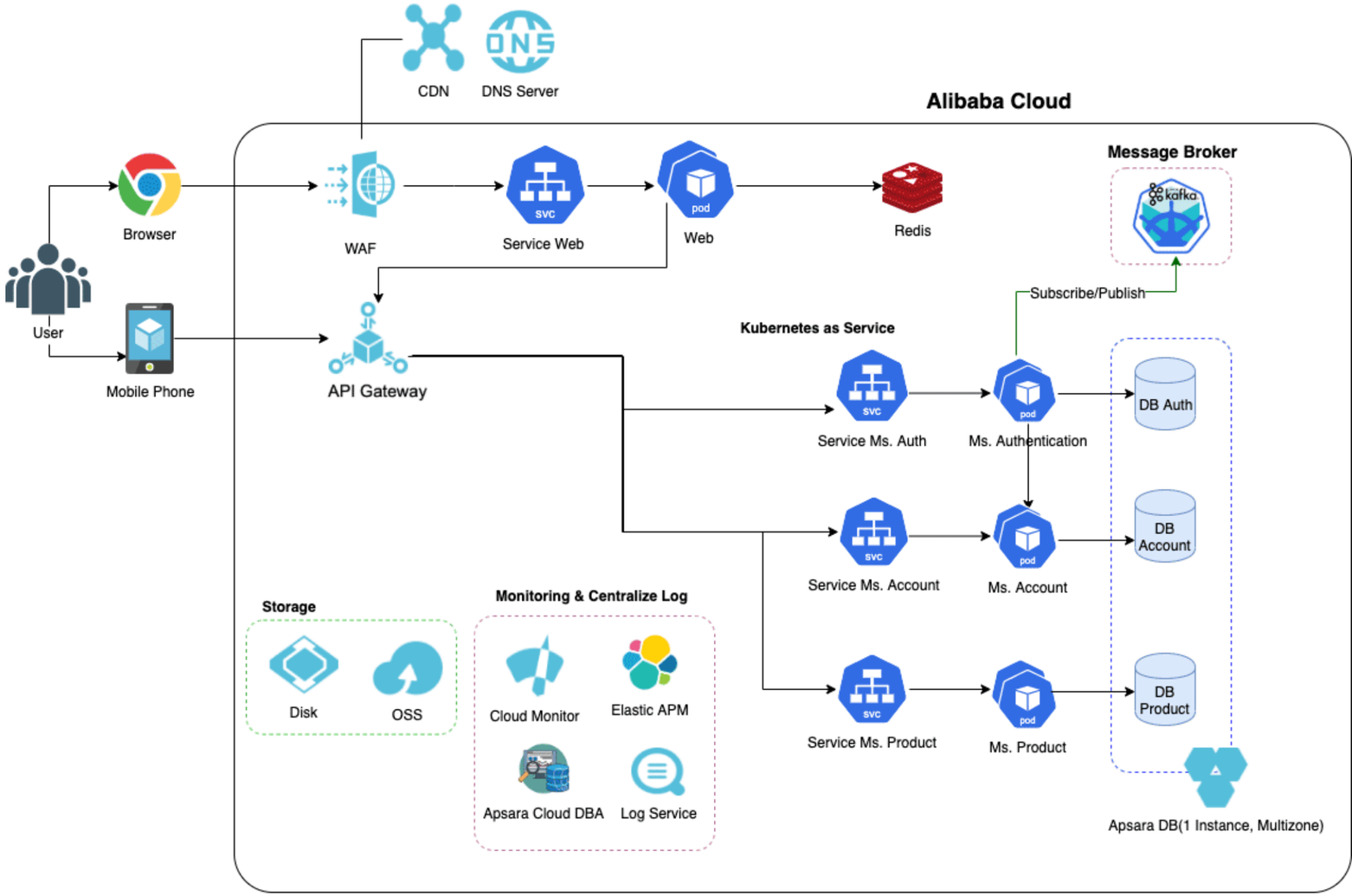
Programming

```
import yfinance as yf

df = yf.download("ETH-USD", start="2020-01-01", end="2022-04-30")
df.tail(10)
```

Date	Open	High	Low	Close	Adj Close	Volume
2022-04-21	3077.829346	3173.451416	2962.410400	2987.480713	2987.480713	20783591093
2022-04-22	2986.938721	3024.854492	2942.358643	2964.835693	2964.835693	16782795477
2022-04-23	2964.802246	2975.322754	2926.740234	2938.114014	2938.114014	9116955609
2022-04-24	2937.347168	2961.882080	2922.128662	2922.732666	2922.732666	9696829579
2022-04-25	2922.990234	3018.415527	2804.507080	3009.393555	3009.393555	22332690614

```python
import json
from datetime import datetime
from hashlib import sha256

class Blockchain(object):
 def __init__(self):
   self.chain = []
   self.chain.append(self.new_block())

  def new_block(self):
   block = {
       'timestamp': datetime.utcnow().isoformat(),
       'prev_hash': self.chain[-1]["hash"] if len(self.chain)>0 else None,
       'nonce': len(self.chain)
   }
   block["hash"]=sha256(json.dumps(block).encode()).hexdigest()
   return block

  def proof_of_work(self):
   while True:
     new_block = self.new_block()
     if new_block["hash"].startswith("0000"):
       break
   self.chain.append(new_block)

bc = Blockchain() #pembuatan rantai blockchain
bc.proof_of_work() #pow untuk menambah blok baru
```

Bagaimana membuat Blockchain di Cloud?



Tugas

Enrol kelas Blockchain di Bisa.ai, kerjakan tugas dan quiz serta kumpulkan sertifikat completion di elearning.bisaai.id