Blockchain Monitoring and Analysis

Prof. James Won-Ki Hong

Distributed Processing & Network Management Lab.
Dept. of Computer Science and Engineering
POSTECH
Pohang, Korea

http://dpnm.postech.ac.kr
jwkhong@postech.ac.kr

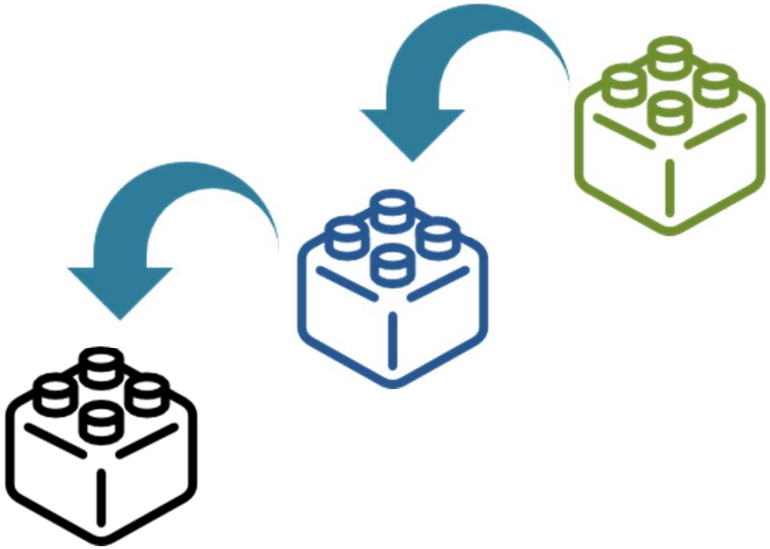
Table of Contents

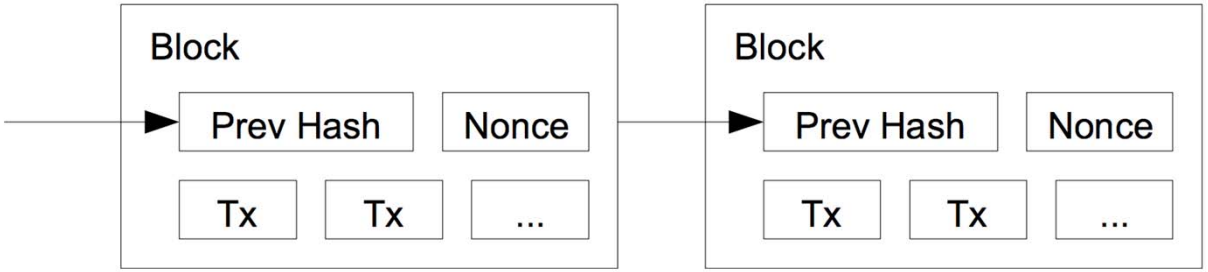
Table of Contents

Bitcoin


Bitcoin Charts
Linear Scale
Log Scale
Zoom 1d 7d 1m 3m 1y YTD ALL
From Apr 29, 2013 To May 19, 2019
$320B
$240B
$160B
$80B
$0
Market Cap
$20,000.00
$15,000.00
$10,000.00
$5,000.00
$0
Price (USD)
24h Vol
20B
0
Jul '13
Jan '14
Jul '14
Jan '15
Jul '15
Jan '16
Jul '16
Jan '17
Jul '17
Jan '18
Jul '18
Jan '19
2014
2015
2016
2017
2018
2019
Market Cap
Price (USD)
Price (BTC)
24h Vol
coinmarketcap.com

- **What is Blockchain?**



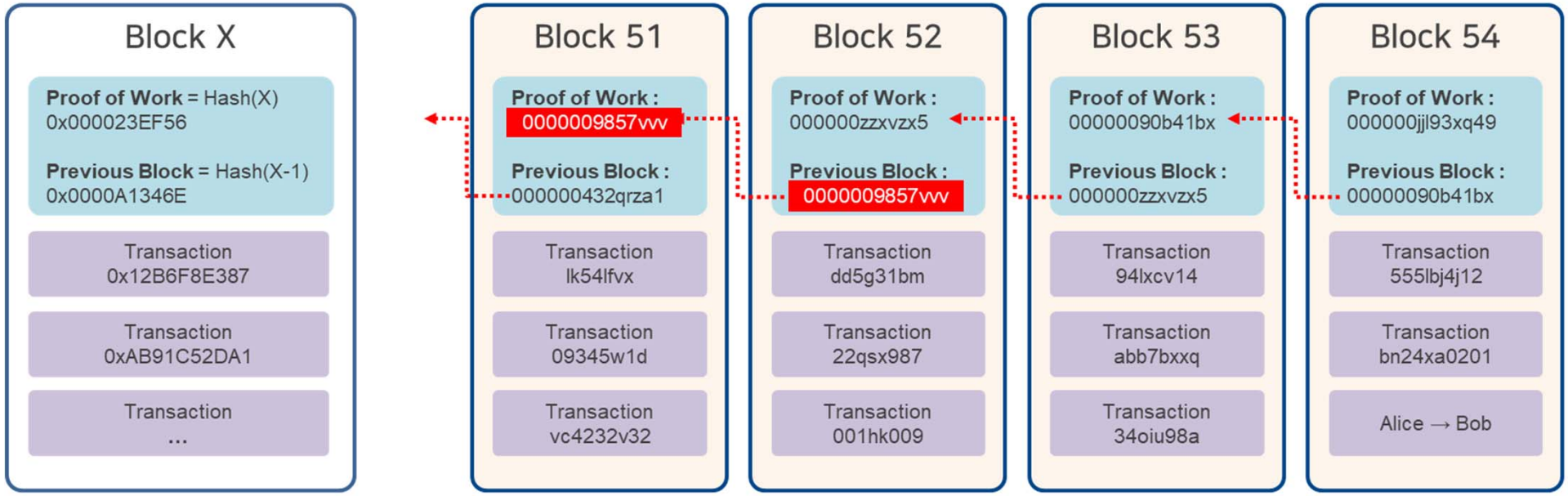


Source: https://bitcoin.org/bitcoin.pdf

Blockchain ≡ Distributed Ledger Technology (DLT)

Introduction to Blockchain

- **Blockchain (= Linked Blocks of Transactions)**

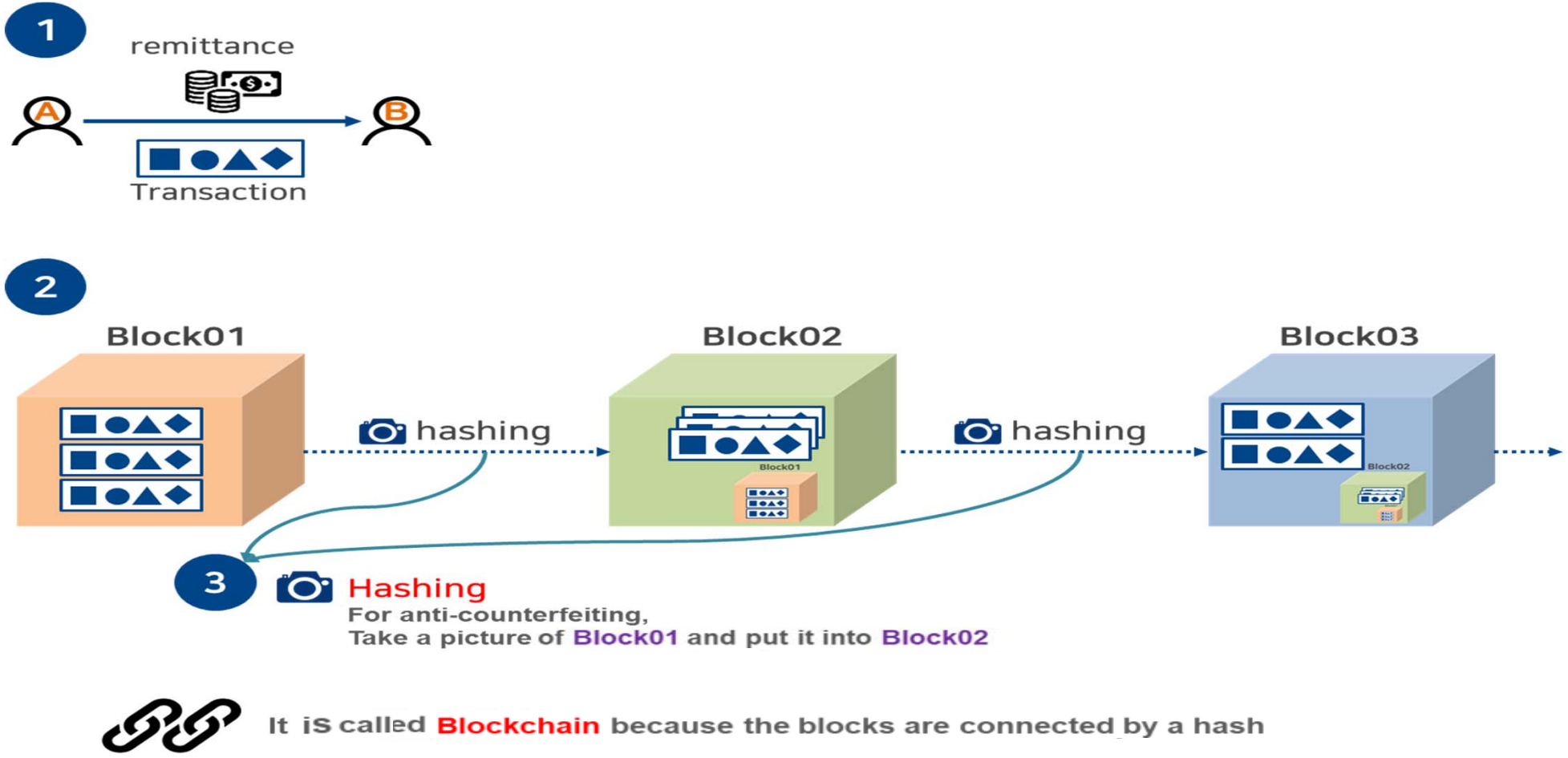


Source: https://www.netguardians.ch/news/2016/12/22/blockchain-explained-part-2

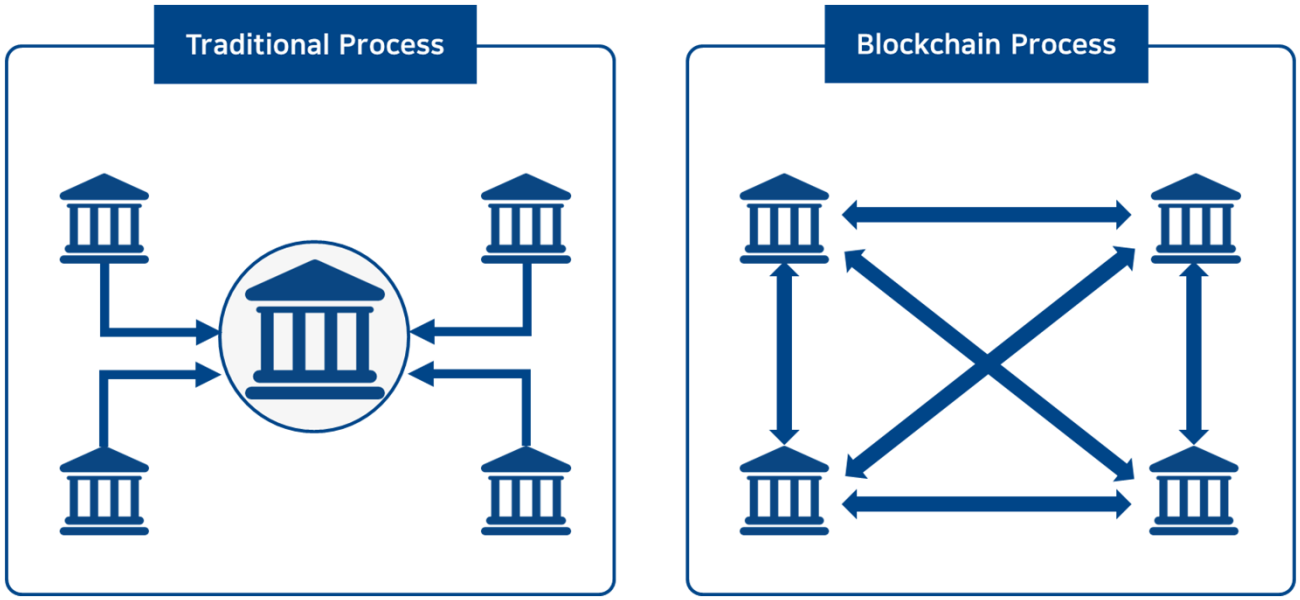
Source: https://fifthperson.com/how-the-blockchain-might-disrupt-the-banking-financial-industries/

Introduction to Blockchain

- **Block creation, Linking Blocks by Hashing**

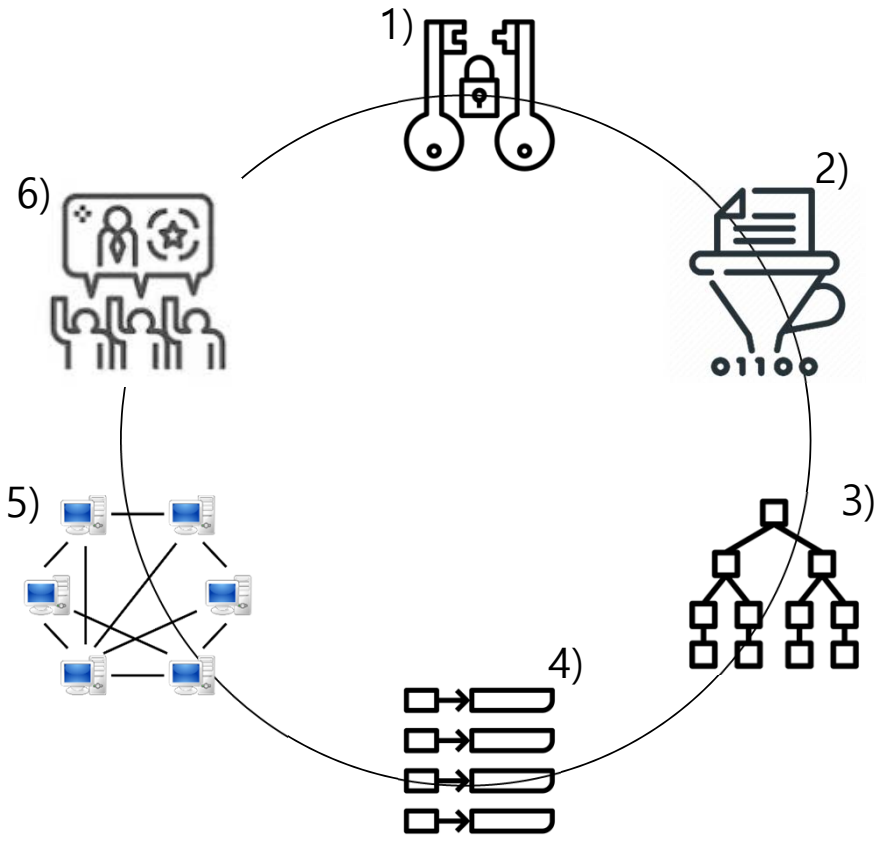


- **Key features of Blockchain**
  1) Decentralized Management
  2) Transparency and Chronology of Transaction Data
  3) Immutability of Transaction Data
  4) Anonymity of Entities ➔ Cause the wrong use of cryptocurrency



source: https://cmp.smu.edu.sg/ami/article/20161208/smarter-banking

- **Key technologies of Blockchain**
  1) Asymmetric Encryption
  2) Hash Function
  3) Merkle Tree
  4) Key-value Database
  5) P2P Communication Protocol
  6) Consensus Algorithm



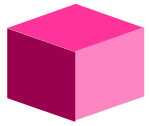
Transaction process in Blockchain

- Transaction → Confirmation → Settlement

1 **Transaction**

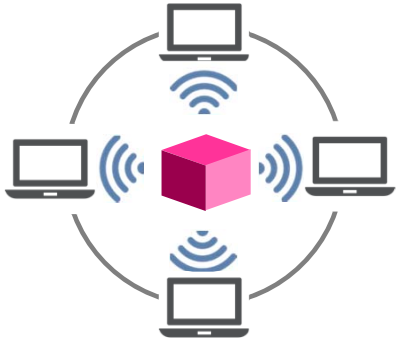
1. A wants to send money to B

2



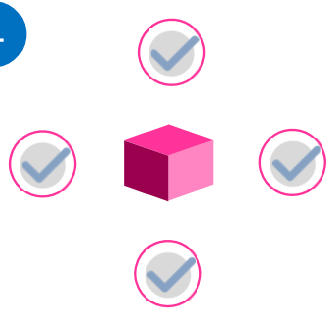
2. The transaction is represented online as a 'block'

3



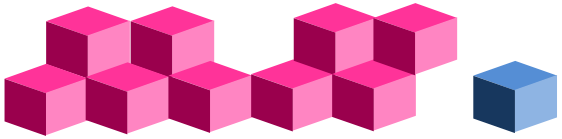
3. The Block is broadcast to every party in the network

4



4. Those in the network approve the transaction is valid

5



Confirmation

5. The block then can be added to the chain, which provides an indelible and transparent record of transactions

6

settlement

6. The money moves from A to B

Public vs. Private Blockchains

Attribute	Permissioned	Non-Permissioned
Private	e.g. Hyperledger Fabric, MS BaaS	-
Public	e.g., Ripple	e.g., Bitcoin, Ethereum

MS BaaS = Microsoft Blockchain as a Service

Introduction to Cryptocurrency

- A cryptocurrency is a digital or virtual currency which is encrypted using cryptography used for the purpose of making payments or representing assets based on Blockchain
  - e.g., Bitcoin, Ethereum, Filecoin
- Altcoins are the various alternative cryptocurrencies that were launched after the massive success achieved by Bitcoin
  - e.g., Ethereum, Litecoin, Bitcoin Cash, Namecoin, Dogecoin, DASH
- Crypto Coins are cryptocurrencies that have been generated by the blockchain to pay for incentives and transactions fees for miners (or block producers)
  - e.g., Bitcoin, Ethereum, Bitcoin Cash, Ripple, DASH, EOS
- Crypto Tokens are cryptocurrencies that have been generated by smart contracts in DApp and represent an asset or utility
  - e.g., Filecoin, Tether, OmiseGO

Cryptocurrencies (Bitcoin and Altcoins)

Crypto-currency	Launch	Aim	Consensus Mechanism	Technological Peculiarities	Privacy	Transactions per Second
Bitcoin (BTC)	01/2009	Purely peer-to-peer version of electronic cash	PoW	UTXO model, 1 MB block size, hash SHA-256, 10 min block time	No	7
Litecoin (LTC)	10/2011	Instant, near-zero cost payments to anyone in the world	PoW	Fork of Bitcoin, decrease of block generation time to 2.5 min	No	56
Ripple (XRP)	09/2012	Real-time gross settlement system, currency exchange and remittance network	Consensus of supermajority	Permissioned, public blockchain	No	> 10.000
DASH	01/2014	Instant, private, secure payments	PoW, Proof of Service	2-tier-network including miners and master nodes	Yes	28
Ethereum (ETH)	07/2015	Smart Contracts for DApps plus electronic payment	PoW	Account, Ethash, decrease of block generation time to 10-20 seconds.	NO	15
Bitcoin Cash (BCH)	08/2017	Lower TX fees and more reliable confirmations than Bitcoin	PoW	Fork of Bitcoin, increase of max. blocksize to 8 MB	No	60

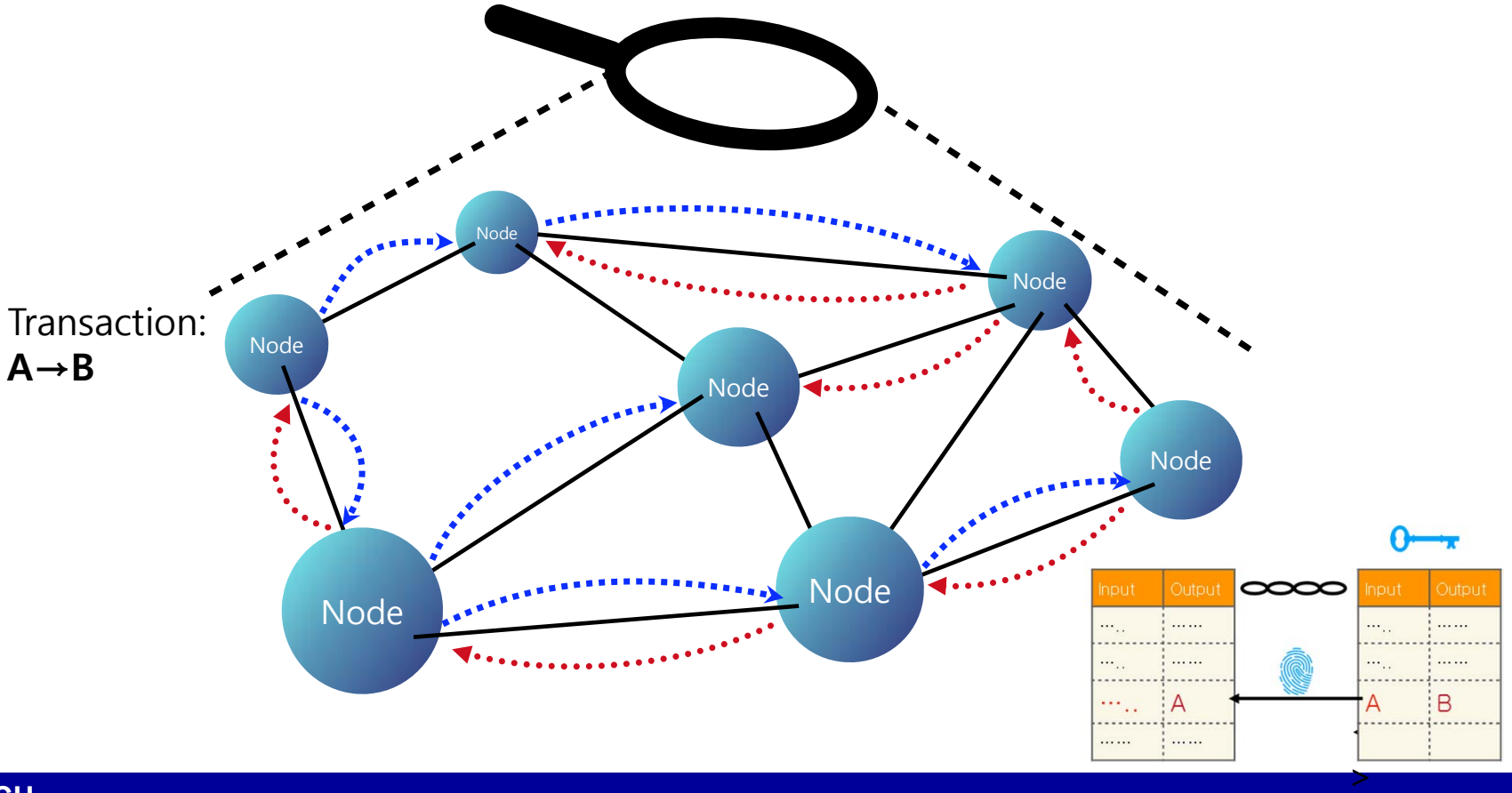
PoW = Proof of Work
PoS = Proof of Stake

Table of Contents

Introduction to Blockchain Monitoring

What is Blockchain Monitoring?

- Overview



Introduction to Blockchain Monitoring

- **Why do we need Blockchain Monitoring? (1)**

BITCOIN NEWS | LAW AND LEGISLATION

Dark Web Drug Dealers Arrested for Laundering $2.3 Mln In BTC

By Alex Korwin - April 17, 2019

source: https://ethereumworldnews.com/dark-web-drug-dealers-arrested-for-laundering-2-3-mln-in-btc/

The criminals were operating out of New York and Texas selling steroids and other controlled substances. | Source: Shutterstock

Bitcoin Laundering: Two NY'ers Convicted in $3 Million Drug-Infused Scam

P. H. Madore 24/04/2019 Bitcoin Crime, Crypto, News

source: https://www.ccn.com/bitcoin-laundering-two-men-convicted/

Why do we need Blockchain Monitoring? (2)

- **Tax compliance**
  - How to impose tax on miners who generate revenue from successively mining blocks and those who receive “airdrops” (National Tax Service)

BITCOIN

Bitcoin can create some sticky tax situations — here’s what experts say investors should do

PUBLISHED FRI, APR 13 2018 • 4:05 PM EDT | UPDATED FRI, APR 13 2018 • 7:00 PM EDT

Evelyn Cheng
@CHENGEVELYN

SHARE

KEY POINTS

- Determining the tax amount on “airdrops” and “hard forks” — which distribute new cryptocurrencies to existing investors — is “an open question,” said Nathan Rigney of The Tax Institute. However, “it’s probably income more similar to a dividend.”
- In the event a taxpayer has created bitcoins or other cryptocurrencies through the “mining” process, the IRS generally considers the profits taxable as self-employment income.
- Since the IRS treats bitcoin as property, online transactions using the cryptocurrency are subject to capital gains tax.

source: https://www.cnbc.com/2018/04/13/how-to-handle-bitcoin-tax-situations-like-airdrops-and-mining.html

Q-8: Does a taxpayer who “mines” virtual currency (for example, uses computer resources to validate Bitcoin transactions and maintain the public Bitcoin transaction ledger) realize gross income upon receipt of the virtual currency resulting from those activities?

A-8: Yes, when a taxpayer successfully “mines” virtual currency, the fair market value of the virtual currency as of the date of receipt is includible in gross income. See Publication 525, *Taxable and Nontaxable Income*, for more information on taxable income.

Q-9: Is an individual who “mines” virtual currency as a trade or business subject to self-employment tax on the income derived from those activities?

A-9: If a taxpayer’s “mining” of virtual currency constitutes a trade or business, and the “mining” activity is not undertaken by the taxpayer as an employee, the net earnings from self-employment (generally, gross income derived from carrying on a trade or business less allowable deductions) resulting from those activities constitute self-employment income and are subject to the self-employment tax. See Chapter 10 of Publication 334, *Tax Guide for Small Business*, for more information on self-employment tax and Publication 535, *Business Expenses*, for more information on determining whether expenses are from a business activity carried on to make a profit.

source: 2014 IRS Tax Guidance

Why do we need the Blockchain Monitoring? (3)

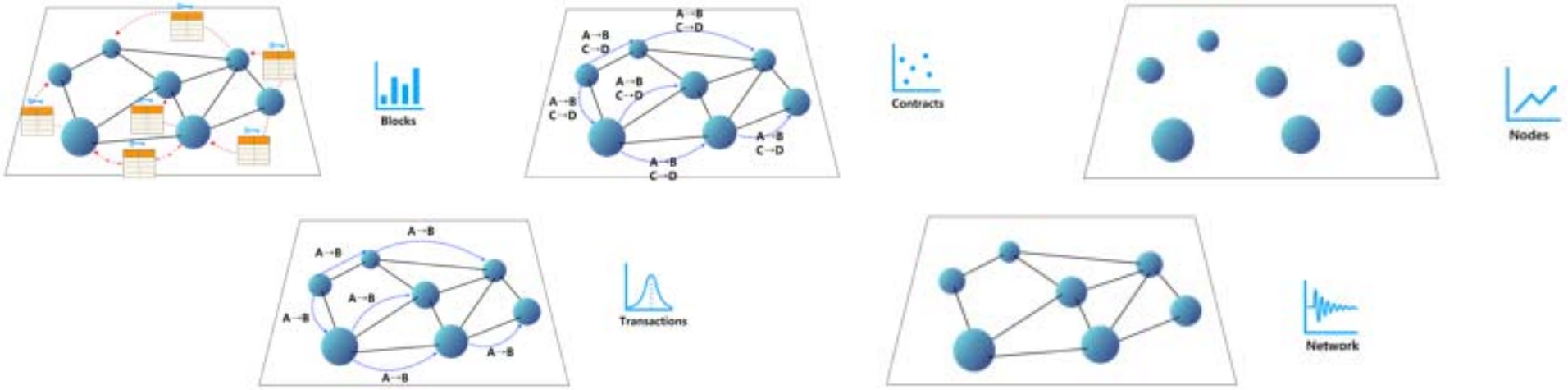
- **DDoS attack**
  - How to detect DDoS attack caused by the big volume of transactions

source: https://news.bitcoin.com/200000-unconfirmed-transactions-pile-another-crazy-day-bitcoin/

- **Others**
  - How to detect vulnerable smart contracts in blockchain
  - How to predict possible events in blockchain
  - How to ensure the availability of blockchain by identifying application and node failures

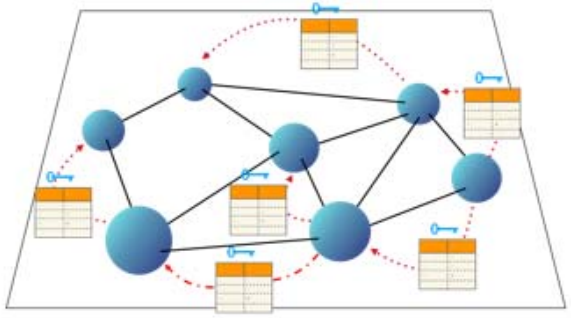
Introduction to Blockchain Monitoring

- **What kind of data should we monitor?**
  - **Block**
  - **Transaction (Historical + Real-time)**
  - **Contract**
  - **Network**
  - **Node**



Introduction to Blockchain Monitoring

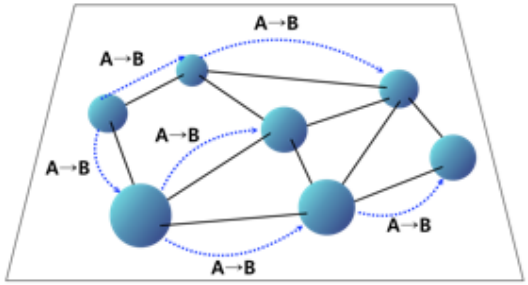
- **Monitoring data: Block**
  - BlockHash, Height, Version, Timestamp, Difficulty, Chainwork, …



  - What can we do? ➔ **Provide the evidence of imposing tax** to miners
    - Calculate how many hashes were consumed for the miner to mine a block
    - Calculate how much the miner earns

Introduction to Blockchain Monitoring

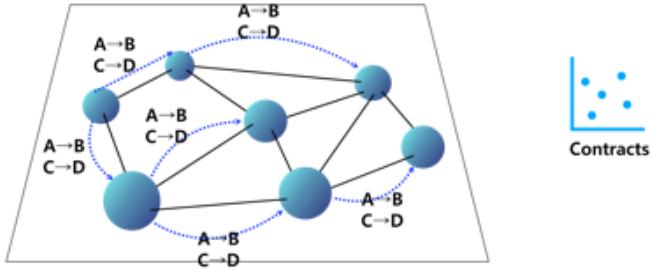
- **Monitoring data: Transaction**
  - Input (Sender Address), Output (Receiver Address), TxHash, Size, Fee, …
  - Mempool state



  - What can we do? ➔ Detect **illegal transactions** and **DDoS attacks**
    - Classify the same user of multiple addresses
    - Build the graph of transaction chain (Who gives and receives)
    - Calculate the rate of incoming and outgoing transactions

Introduction to Blockchain Monitoring

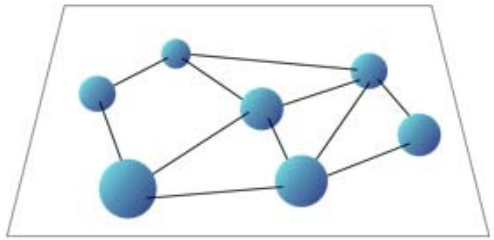
- **Monitoring data: Smart Contract**
  - Contract Address, State, Bytecode, Language, Event, …



  - What can we do? ➔ **Protect from being hacked**
    - Detect vulnerabilities that can appear from smart contracts
    - Tract the state and activity of the designated smart contract

Introduction to Blockchain Monitoring

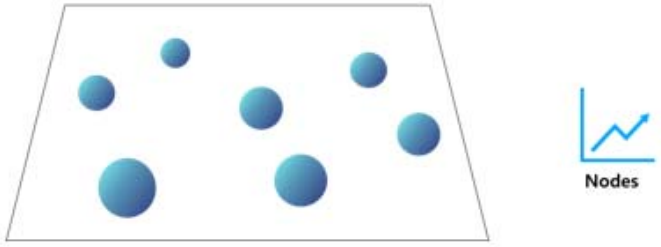
- **Monitoring data: Network**
  - Peer Connectivity, Throughput, Latency, Bandwidth, …



  - What can we do? ➔ **Analyze performance and scalability** of blockchains
    - Analyze characteristics of propagation of blocks and transactions
      - Propagation delay between nodes
      - Performance per network connection and node type
    - Measure performance on broadcasting routing
      - The amount of duplicate messages
      - Comparison of routing performance per each blockchain platform

Introduction to Blockchain Monitoring

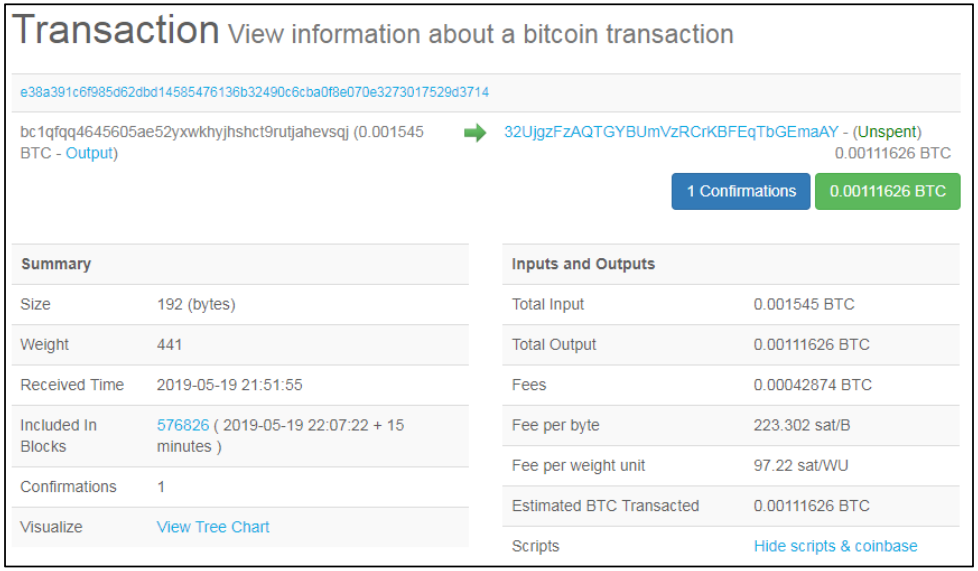
- **Monitoring data: Node**
  - Node Type, CPU & Memory Usage (CPU, Mem, Disk), Sys. Info, …

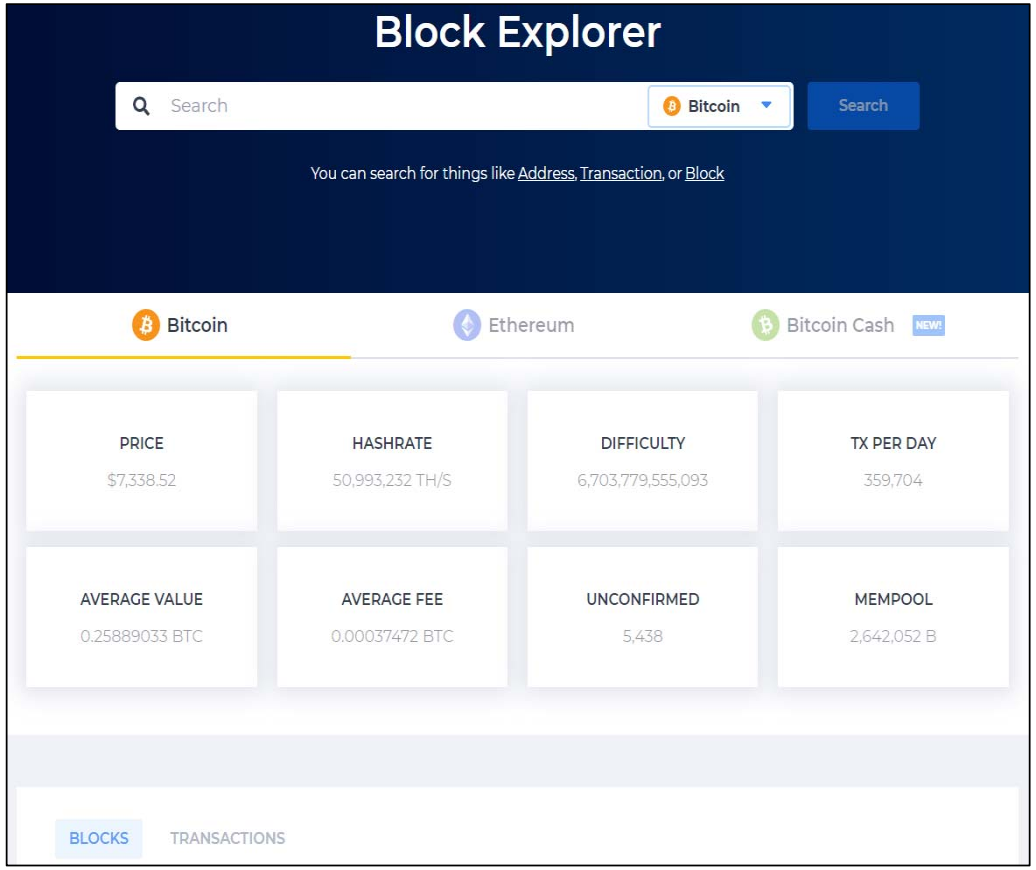


  - What can we do? ➔ **Manage "private blockchains"**
    - Measure system failure and performance of nodes
      - Resource state of nodes, program error, system/network performance

Introduction to Blockchain Monitoring

- **Methods to collect data (1)**
  - **Using Blockchain Explorer**
    - https://www.blockchain.com/explorer
    - https://blockexplorer.com/
    - https://etherscan.io/
    - …





source: https://www.blockchain.com/explorer

Introduction to Blockchain Monitoring

- **Methods to collect data (2)**
  - **Using RPC on blockchain clients**

```
bitcoin-cli help
== Blockchain ==
getbestblockhash
getblock "blockhash" ( verbosity )
getblockchaininfo
getblockcount
getblockhash height
getblockheader "hash" ( verbose )
getchaintips
getchaintxstats ( nblocks blockhash )
getdifficulty
getmempoolancestors txid (verbose)
getmempooldescendants txid (verbose)
getmempoolentry txid
getmempoolinfo
getrawmempool ( verbose )
gettxout "txid" n ( include_mempool )
gettxoutproof ["txid",...] ( blockhash )
gettxoutsetinfo
preciousblock "blockhash"
pruneblockchain
savemempool
verifychain ( checklevel nblocks )
verifytxoutproof "proof"

== Control ==
getmemoryinfo ("mode")
help ( "command" )
logging ( <include> <exclude> )
stop
uptime
```

Bitcoin RPC commands

```
bitcoin-cli getblock 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
{
  "hash": "000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f",
  "confirmations": 539458,
  "strippedsize": 285,
  "size": 285,
  "weight": 1140,
  "height": 0,
  "version": 1,
  "versionHex": "00000001",
  "merkleroot": "4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b",
  "tx": [
    "4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b"
  ],
  "time": 1231006505,
  "mediantime": 1231006505,
  "nonce": 2083236893,
  "bits": "1d00ffff",
  "difficulty": 1,
  "chainwork": "0000000000000000000000000000000000000000000000000000000100010001",
  "nTx": 1,
  "nextblockhash": "00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048"
}
```

The result of a RPC command to get information of a block

Introduction to Blockchain Monitoring

- **Methods to collect data (3)**
  - **Parsing the log of blockchain clients**

```
UpdateTip: new best=000000000000000027aa250952750129386 9c6e00773d7ea267da9be7ad5e0 height=572949
UpdateTip: new best=000000000000000000657fa3867bfebc0aeb93446942c936d44b9c3173efdda height=572950
UpdateTip: new best=000000000000000001192b5f0ad5cca9606cd1558e0c8a399dcdab061bc6543 height=572951
UpdateTip: new best=000000000000000001b1c0595c6be65fed7e3bab5d762f8757629deef408734 height=572952
UpdateTip: new best=000000000000000000125bfc8911bc85b0dd631e94853b4806257a5c6121813b height=572953
UpdateTip: new best=000000000000000000002df42a617c92514cdc4d53bba0252f756d52286463939 height=572954
UpdateTip: new best=000000000000000001df69225c15636339c9f9681dce17cfae4176f9031a08a height=572955
```

.
.
.

Logs generated from Bitcoin Core

Introduction to Blockchain Monitoring

- **Methods to collect data (4)**
  - **Developing a small client**
    - Using **socket library** and **each protocol**

inv

Allows a node to advertise its knowledge of one or more objects. It can be received unsolicited, or in reply to *getblocks*.

Payload (maximum 50,000 entries, which is just over 1.8 megabytes):

Field Size	Description	Data type	Comments
1+	count	var_int	Number of inventory entries
36x?	inventory	inv_vect[]	Inventory vectors

getdata

getdata is used in response to inv, to retrieve the content of a specific object, and is usually sent after receiving an *inv* packet, after filtering known elements. It can be used to retrieve transactions, but only if they are in the memory pool or relay set - arbitrary access to transactions in the chain is not allowed to avoid having clients start to depend on nodes having full transaction indexes (which modern nodes do not).

Payload (maximum 50,000 entries, which is just over 1.8 megabytes):

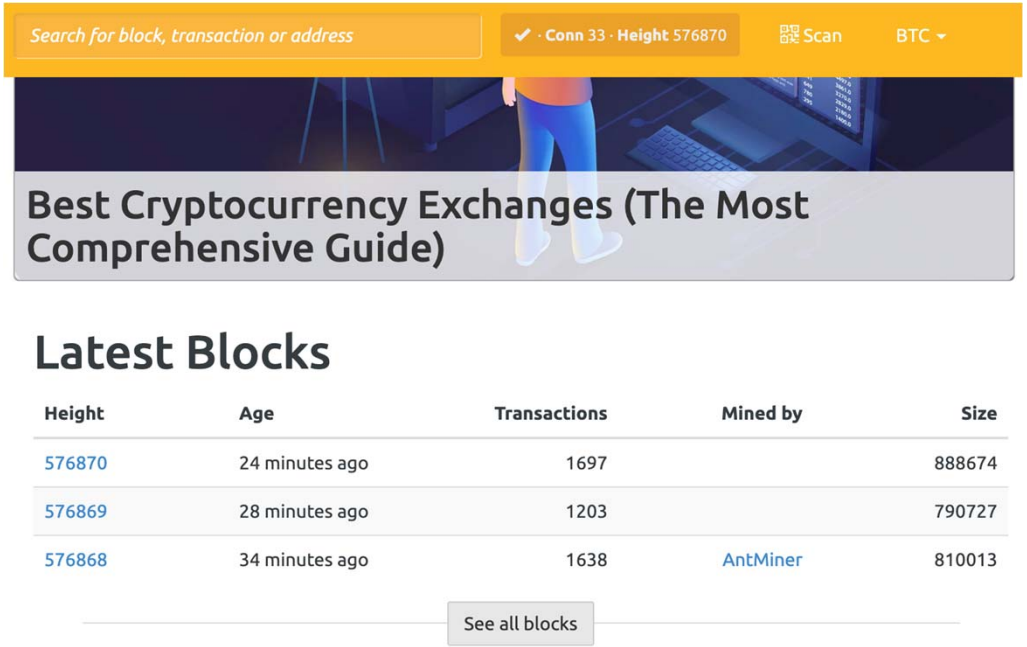
Field Size	Description	Data type	Comments
1+	count	var_int	Number of inventory entries
36x?	inventory	inv_vect[]	Inventory vectors

source: Bitcoin Protocol Documentation,
https://en.bitcoin.it/wiki/Protocol_documentation

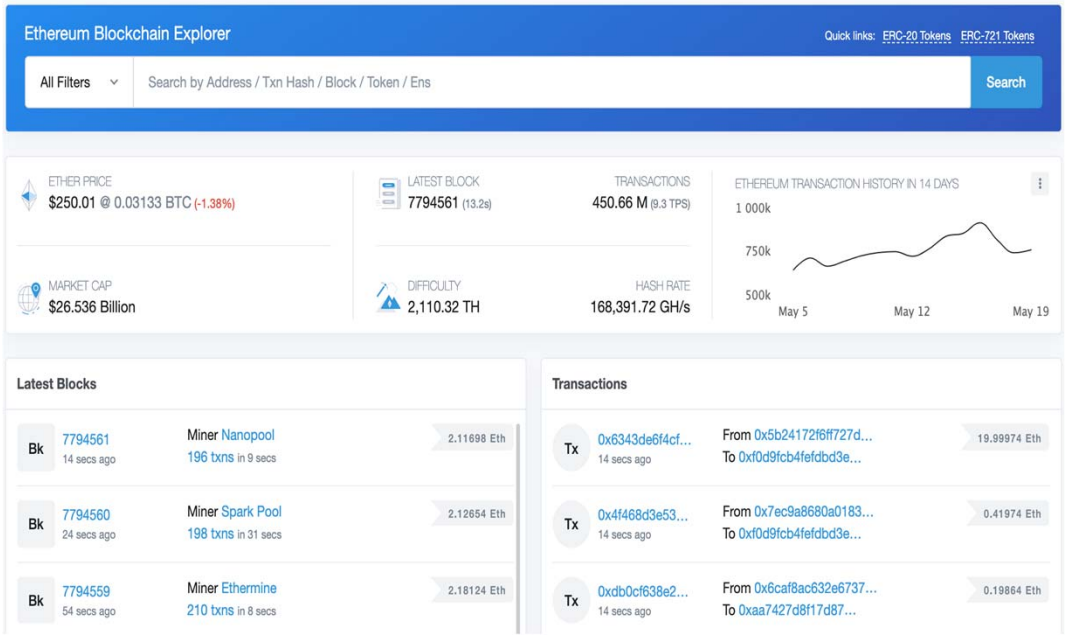
Table of Contents

Blockchain Monitoring and Analysis System

- **Related Work (1)**
  - **Blockchain Explorer – Bitcoin, Ethereum, …**
    - Show the blockchain data such as Block, Transaction and Contract



Source: Blockexplorer – Bitcoin, https://blockexplorer.com/

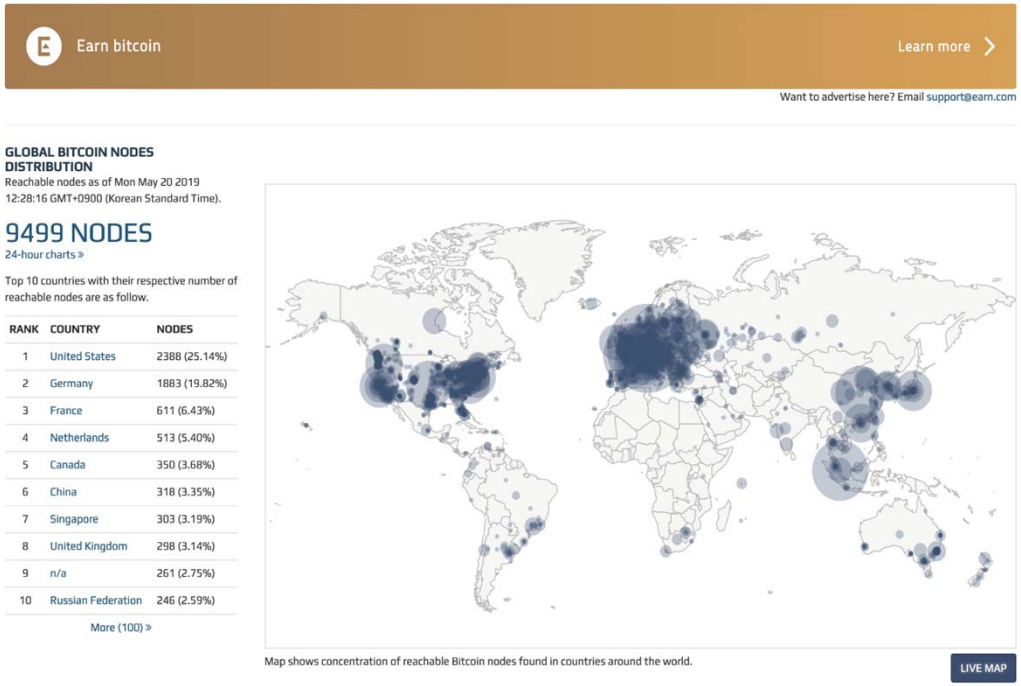


Source: EthereScan – Ethereum, https://etherscan.io/

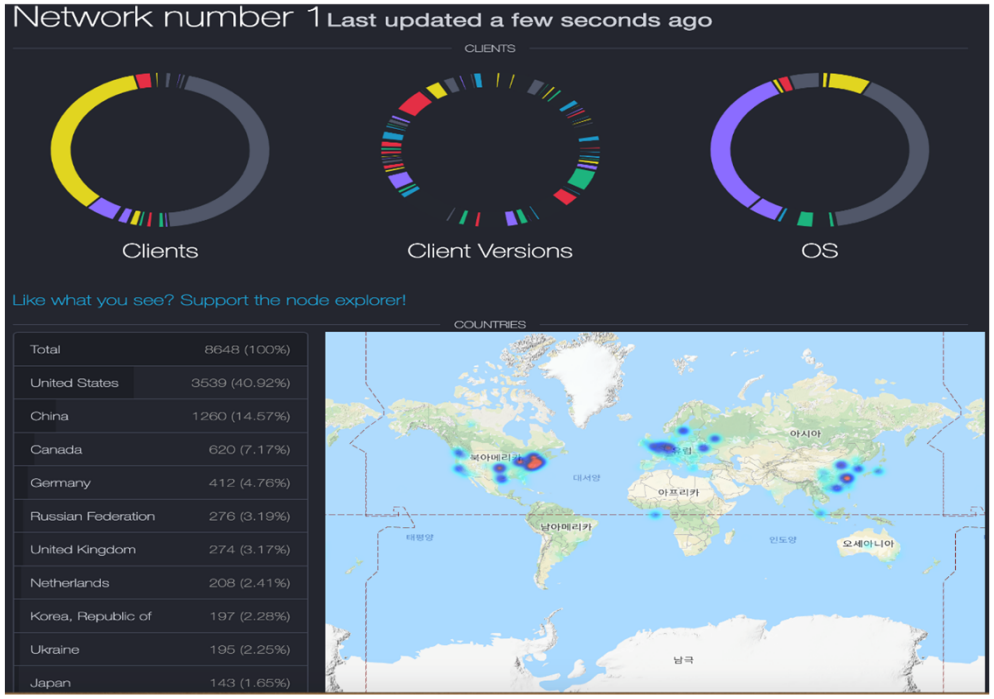
Blockchain Monitoring and Analysis System

- **Related Work (2)**
  - **Blockchain Nodes – Bitcoin, Ethereum, …**
    - Show the overall information of nodes in blockchain network

      Ex) The number of nodes, Geographical position of nodes



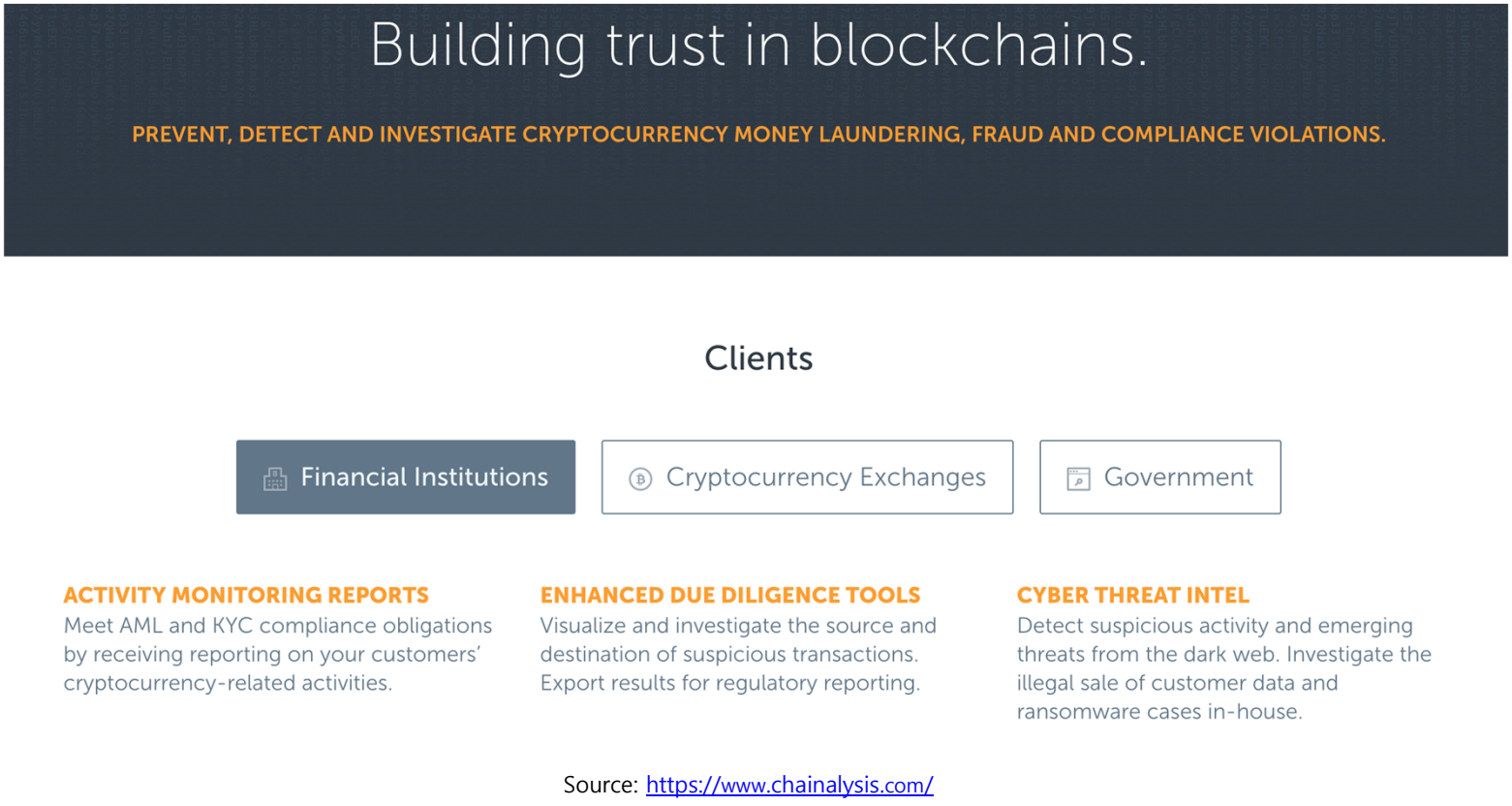
Source: https://bitnodes.earn.com/



Source: https://www.ethernodes.org/network/1

Blockchain Monitoring and Analysis System

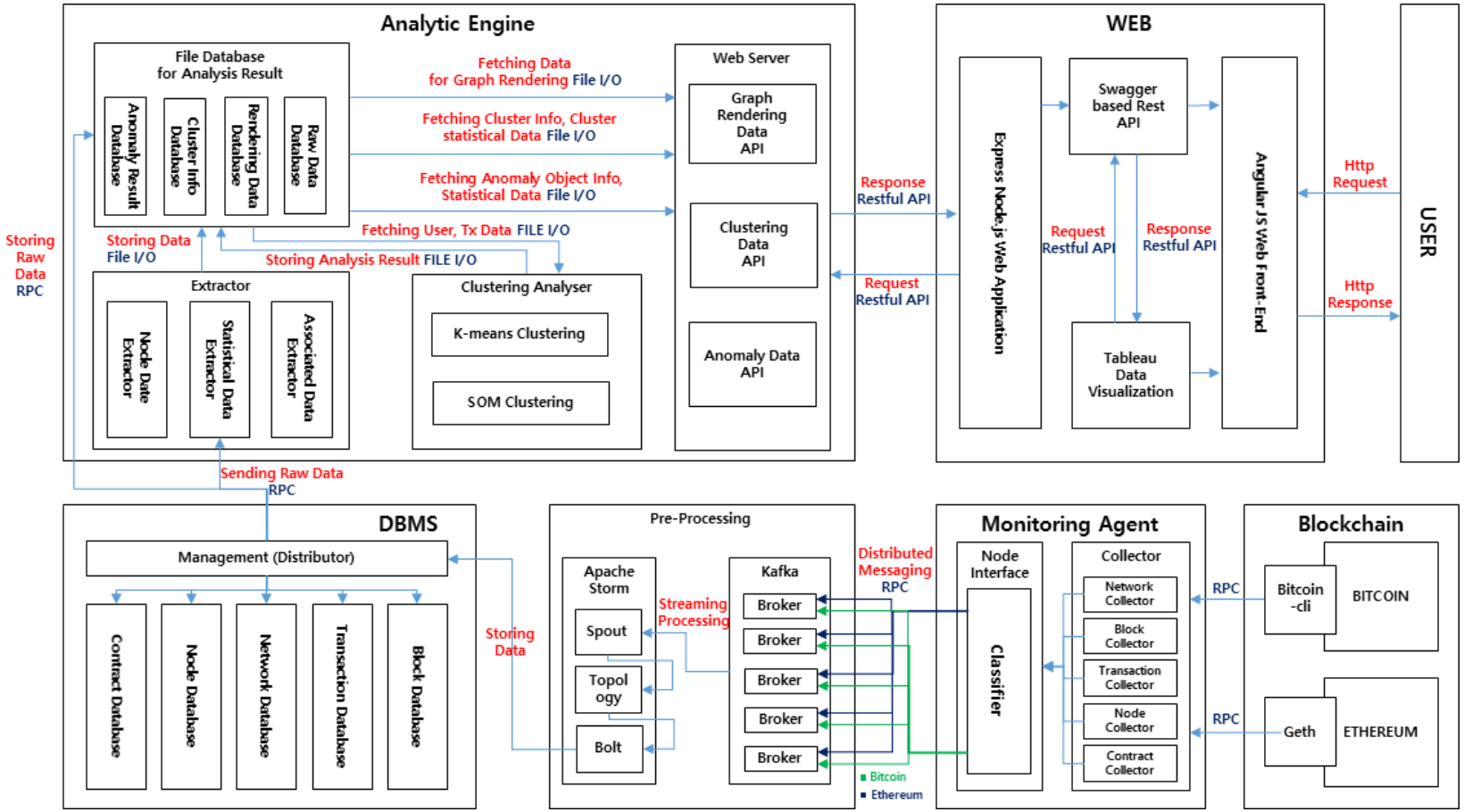
- **Related Work (3)**
  - **Blockchain Analysis – CHAINALYSIS**



Source: https://www.chainalysis.com/

Blockchain Monitoring and Analysis System

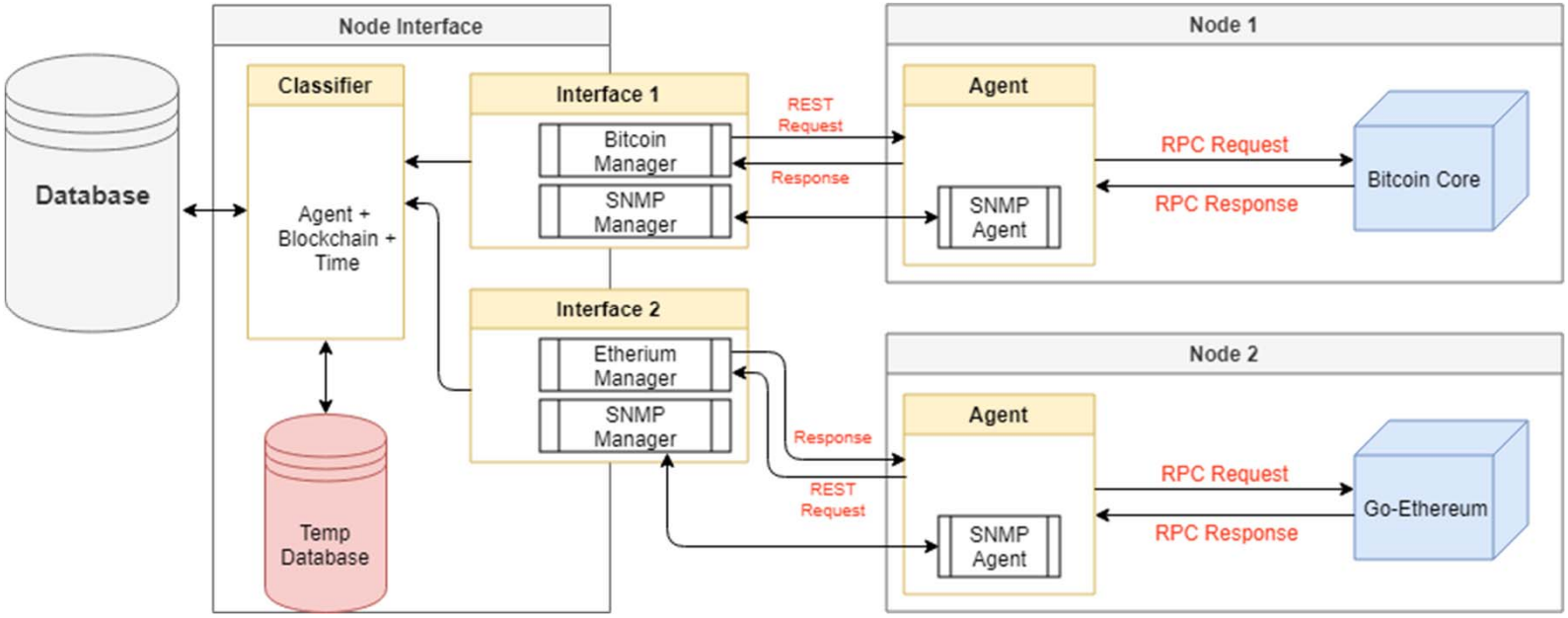
- **Overall Architecture – our own**



Blockchain Monitoring and Analysis System

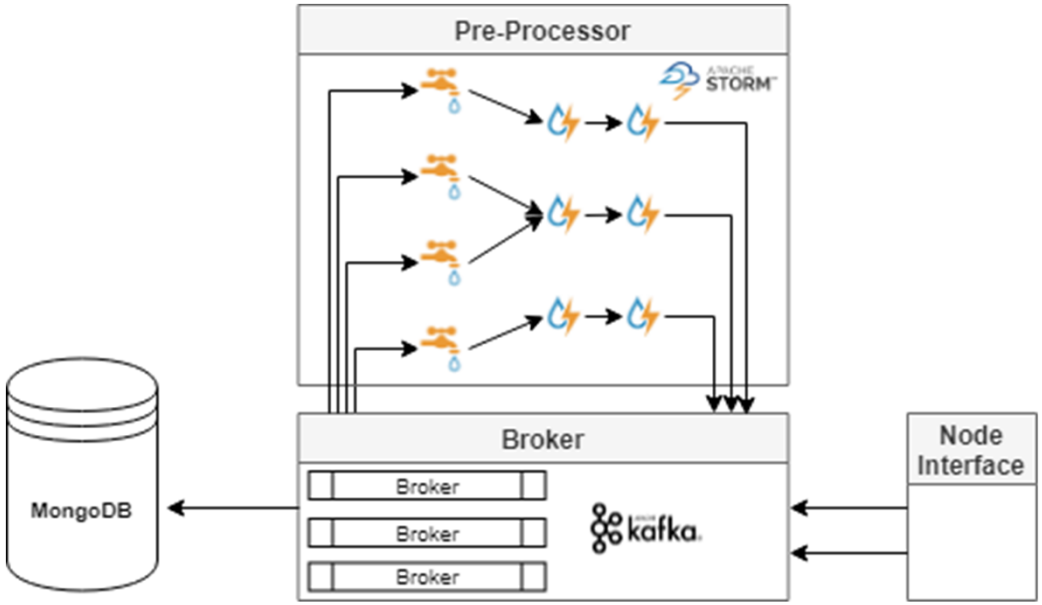
▪ Monitoring Agent & Node Interface

- **Collect data by using RPC on blockchain platforms**
  - Node, Network, Block, Transaction, Contract



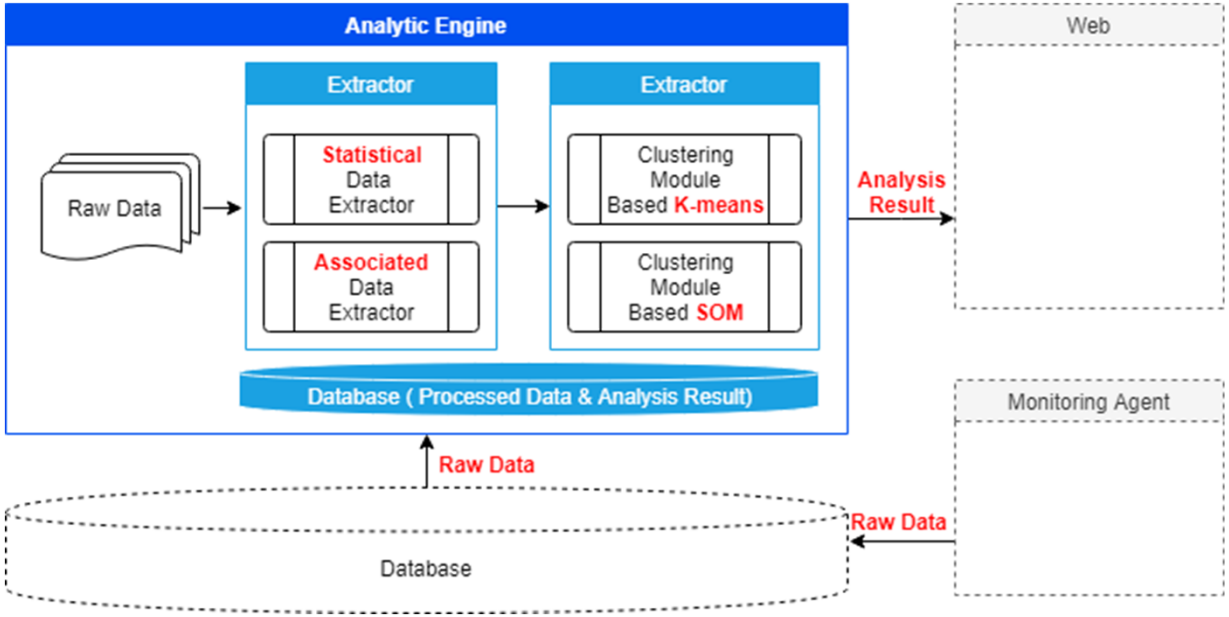
Blockchain Monitoring and Analysis System

- **Database on Blockchain server**
  - **Receive the collected data through Kafka broker**
    - To store a huge real-time data such as a number of pending transactions from several nodes
  - **Preprocess the received data using Apach storm**
    - Indexing, extraction of statistical information, separating transactions from a block, distribution on storing data



Blockchain Monitoring and Analysis System

- **Analysis engine on Blockchain server**
  - **Extract statistical data and associated data**
    - Analysis engine for time-series analysis, processing on statistical data and association rule between data
  - **Analyze the association data through clustering algorithm**
    - K-means, SOM



Blockchain Monitoring and Analysis System

- **Web Interface Architecture**
  - Show the collected data and result of analysis (Visualization processing)
  - Support REST APIs to allow users to get the data

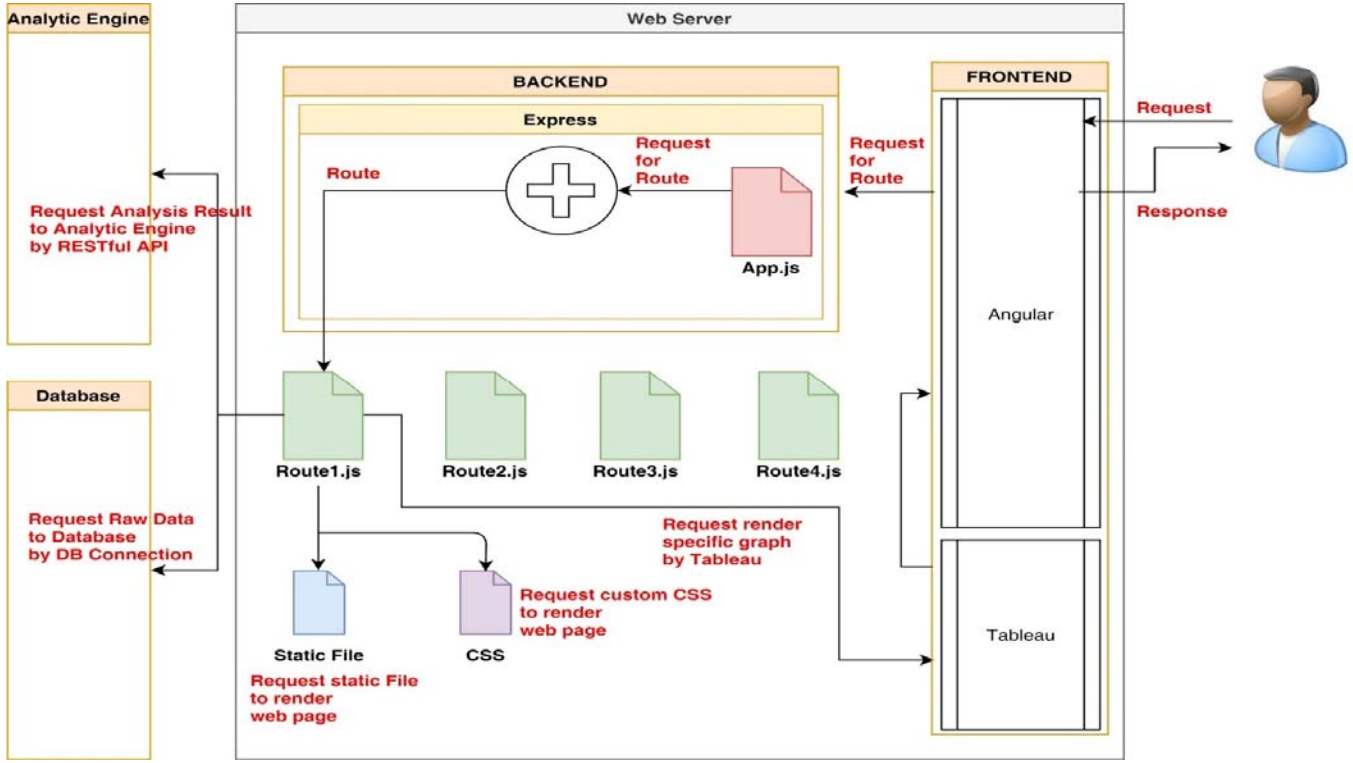


Table of Contents

Applications & Summary

- **Applications**
  - **Blockchain Forensic**, **Criminal Transaction Detection**, **DDoS Protection**, **Private Blockchain Management**, etc.

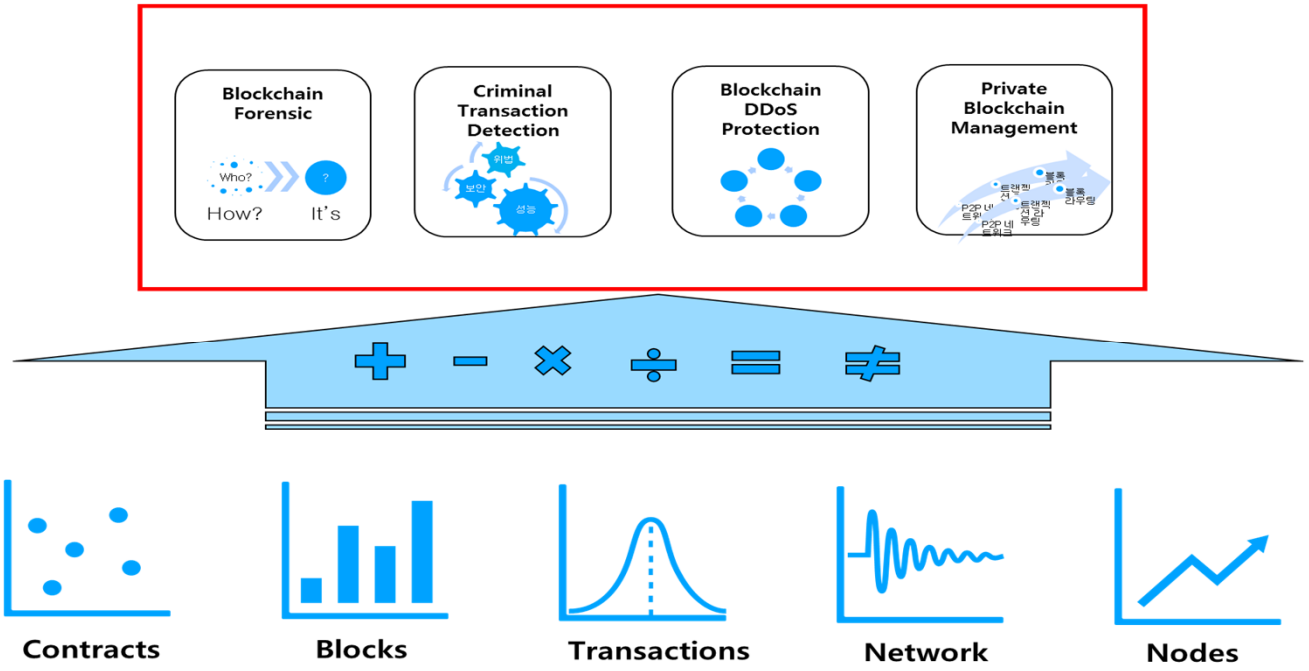


Table of Contents

Summary

- **Blockchain**
  - Main features: Decentralization, Transparency, Immutability, Anonymity
- **Needs of Blockchain Monitoring**
  - illegal transaction detection, DDoS attack detection, tax imposition of revenue from mining, ...
- **Monitoring data**
  - Block, Transaction, Smart Contract, Network, Node
- **Blockchain Monitoring and Analysis System**
- **Applications**
  - Blockchain Forensic, Criminal Transaction Detection, Blockchain DDoS Protection, Private Blockchain Management

References

- http://dpnm.postech.ac.kr/cs490u/
- http://www.postechx.kr/ko/school/2018fall/courseware/50562
- http://blockchain.postech.ac.kr/
- https://ethereumworldnews.com/dark-web-drug-dealers-arrested-for-laundering-2-3-mln-in-btc/
- https://www.ccn.com/bitcoin-laundering-two-men-convicted/
- https://www.cnbc.com/2018/04/13/how-to-handle-bitcoin-tax-situations-like-airdrops-and-mining.html
- https://news.bitcoin.com/200000-unconfirmed-transactions-pile-another-crazy-day-bitcoin/
- https://www.blockchain.com/explorer
- https://blockexplorer.com/
- https://etherscan.io/
- https://en.bitcoin.it/wiki/Protocol_documentation


Q & A