- T A O -

Hybrid Blockchain Architecture Consensus for IoE and AI Creativity

2018. TokenizeIT Conference Material

2018. 09. 10

CEO : KT Ahn

+82-(0)10-2677-5554

cpplover@trustfarm.net
admin@tao.foundation

1. Executive Summary

Subject : How to solve big industry problem?

Problems::

■ **1. Privacy : Centralized IoT Systems Hard to Cover Security of Privacy.**

■ **2. Fairness : Contents industry has problem of Fairness of contents creator, consumer, dominant platform providers**

■ **3. Infra Monopoly : Deep Learning Infra needs to very big investment. So, School or Small, of mid-level enterprise has barrier of new emerging technology.**

◎ **Answer :**

1) Needs Shareable Economy with Smart Contract Applied on IoE devices.
   -> It will solve M2M value swapping and pay without intermediates system or middleman.
   -> It will solve privacy problem, examples, doorkey sharing in AirBnB systems, with DeCentralized Apps

2) Contents Creator get more revenue compared than current contents industry rewards, and also promoter and listener (consumer) also get rewards, It means reward system will be more fair and Creator's copyright will be more secured and traceable easily.

3) Deep Learning infra resource crowd marketplace will solve research barriers, it is shareable economy on using infra.
   -> Overall very expensive GPU cluster investor also get effective revenue, and anonymous data provider also get rewards, Researcher will using infra cheaper, and sell their research to who want to use.

■ **Effects :**

In all industry , We can directing the current industries big problem, "The Rich get Richer, The Poor get Poorer", Applying Fair Consensus for Participants, more consume and more anonymous contributors makes more Industry Pie, it will shared all participants.
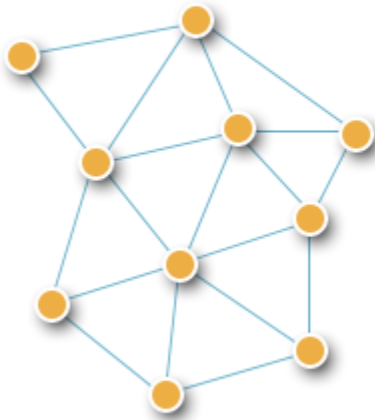
More Fair distributions, Technical backend will be used with Emerging blockchain Technology.

Most important things, How to share , make FAIR CONSENSUS for all participants.

1. Differences between Central vs DeCentral/Distributed System?
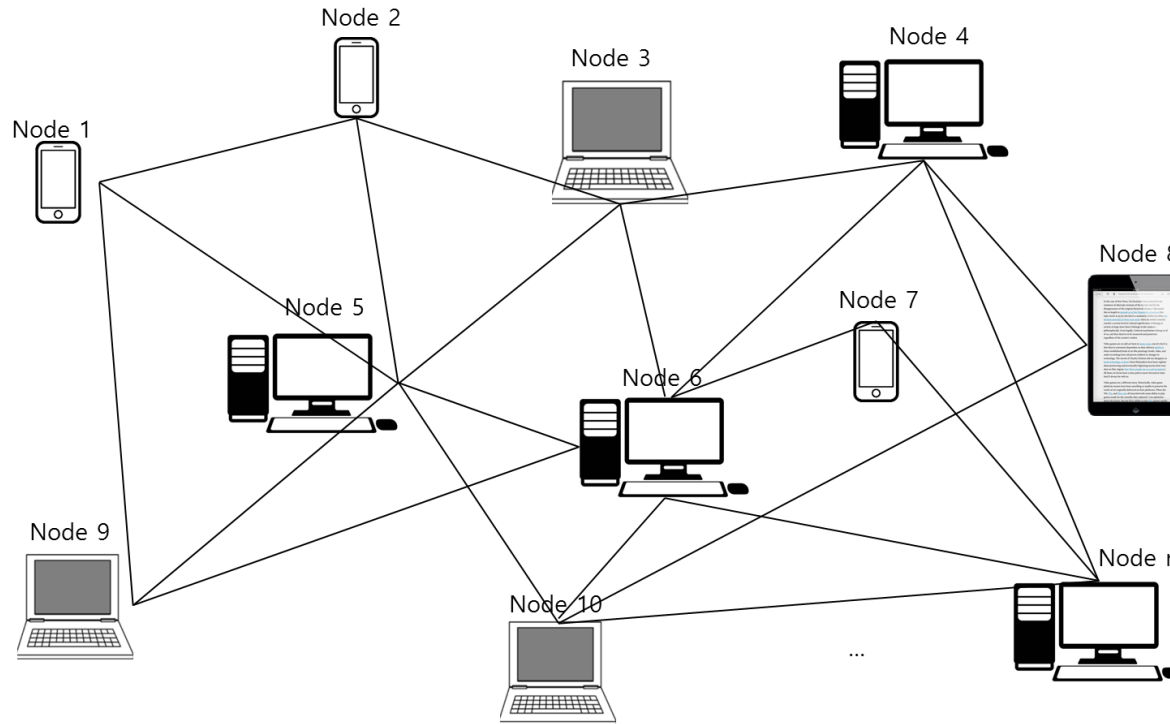
Distributed

Centralized

Decentralized

Starting of Internet : 1960~80s : P2P connected , Poor Connectivity
Recent Internet : 90S ~ Now : Dominant Centralized , little Distributed
From Now on ~ : Hybrid [DeCentralized/Distributed, Centralized]

1-1. Peer2Peer network node diagram

◈ **BLOCK : A SET OF TRANSACTIONS – Transaction includes each contracts**
▶ In Full capable nodes : Each Node stores blockchain datas.
▶ In Semi-Full capable nodes : Node stores recent blockchain datas.(for saving storage)
▶ In Lite capable nodes : Node stores recent blockchain datas. or just doing what it needing transactions.
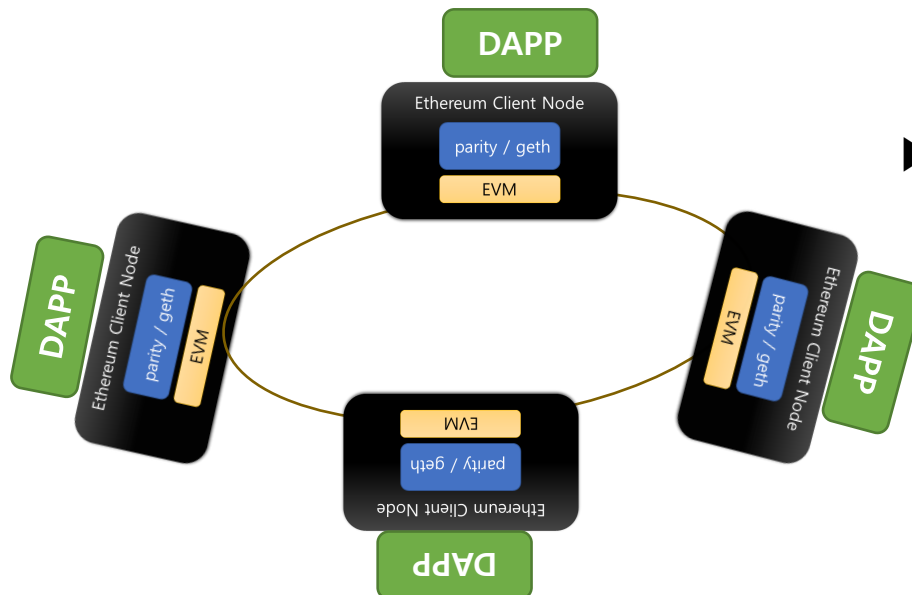
3. How to apply SmartContract and DApp?

DApp is run on all participatants node.
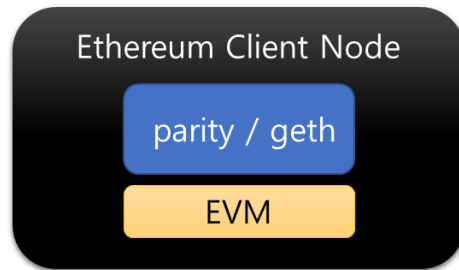
▶ **Popular SmartContract Capable Ethereum Client node.**
   Node composited :
   - P2P Network protocol stack dispatcher
   -   Block/Transaction Verifier , BlockDB Storage Manager
   -   DAPP/SmartContract Execution EVM(VirtualMachine)

▶ **DAPP run on BTW Nodes.**
   OPCode (Operation Instruction Machine Code)
   DAPI (HighLevel Language API, or Keyword)
   - Nodes do same contract execution:
   - Depends on OP Code DAPI,
     It is executed on Local Node.
     (Most ReadOnly OP, DAPI)

4. Current Blockchain (Ethereum)Scalability problem?

- ▶ **Beside of Powerful Contract Machine, current issues are Scalablities**
    - From 2016, There's Heavy transaction and Contract SPAM DDOS and Several Contract Attack Makes Ethereum Network to serious traffics.
    - Preventing the Contract SPAM DDOS, DApp Gas Prices (Execution/Transaction Fee) has increased, and Expensive now.
    - Several Popular DAPPS makes many of transactions pendings. Recent days, over 30K TX has pending.
    - It Makes TX Fee price high. [2017.12: $3 /NormalTX/ETH $1200USD]
    - Full chain Size has increased exponentially **[2017.11 : 350GB , 2018.1 : 550GB , 2018.09 : 1.5TB]**

- ▶ **Approach to Solve in DevSide.**
    - Change Main algorithm to POS (Proof of Stake)
    - Side Chain Development.
    - ..
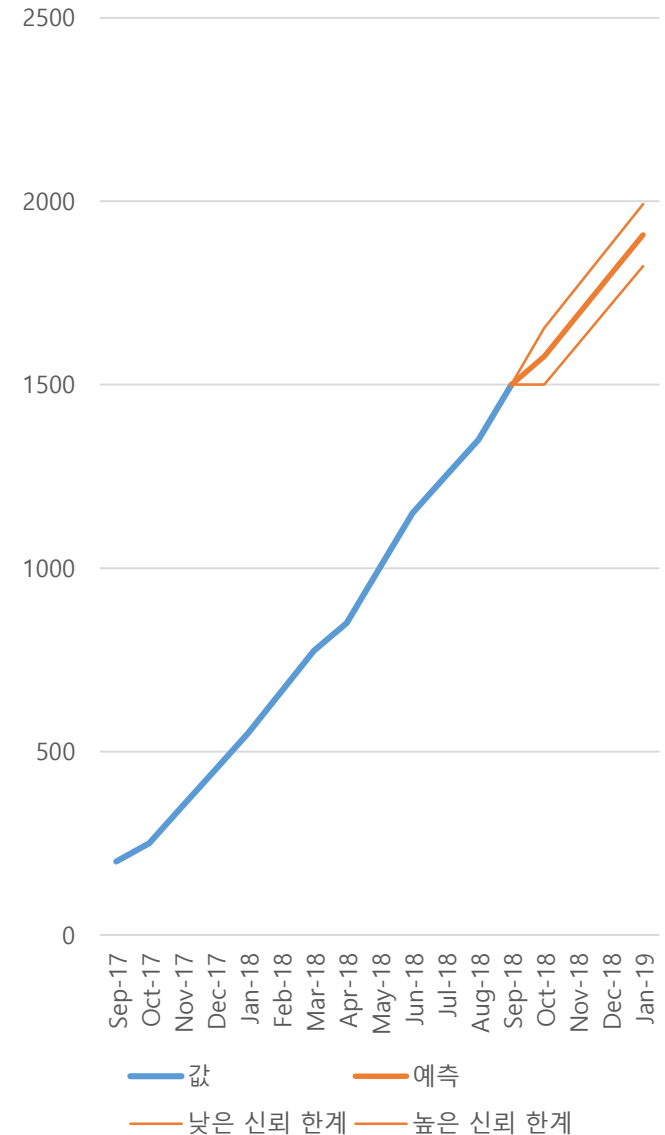
5. Current SmartContract (EVM) Engine problem?

- ▶ **Beside of Powerful Contract Machine, Spend High Computing Resources**
  - From 2016, There's Heavy transaction and Contract SPAM DDOS and Several Contract Attack Makes Ethereum Network to serious traffics.
  - At that time, client nodes needs **over 16GB memory and Heavy IO Requests**.
    Fast SSD (Solid State Drive) is needs on Recent days.
  - It is caused high-level abstracted machine instruction set.

- ▶ **Approach to Solve in DevSide.**
  - WASM (WebAssembly) is researching.
  - Lite Client researching.

6. Alternatives of Current Blockchain tech.

- **▶ Scalable issue solving tech – Overall Blockchain industry**
  - Offline Side chain development.
  - TPS increasing method development. – <u>Layer-2 Tech</u>
  - DPOS (Delegated Proof-of-Stake) enhancement.
  - Chain Pegging and Interblockchain communication method.
  - TAO-Blockchain Router

- **▶ Blockchain interconnect solving tech – Overall Blockchain industry.**
  - Atomic Swap
  - Contract Message Driven Interchange
  - DEX (DeCentralized Exchange)
  - Bridging the Blockchain.
  - Gatewaing tech the heterogeneous blockchain.
  - TAO-Uses above method hybrid
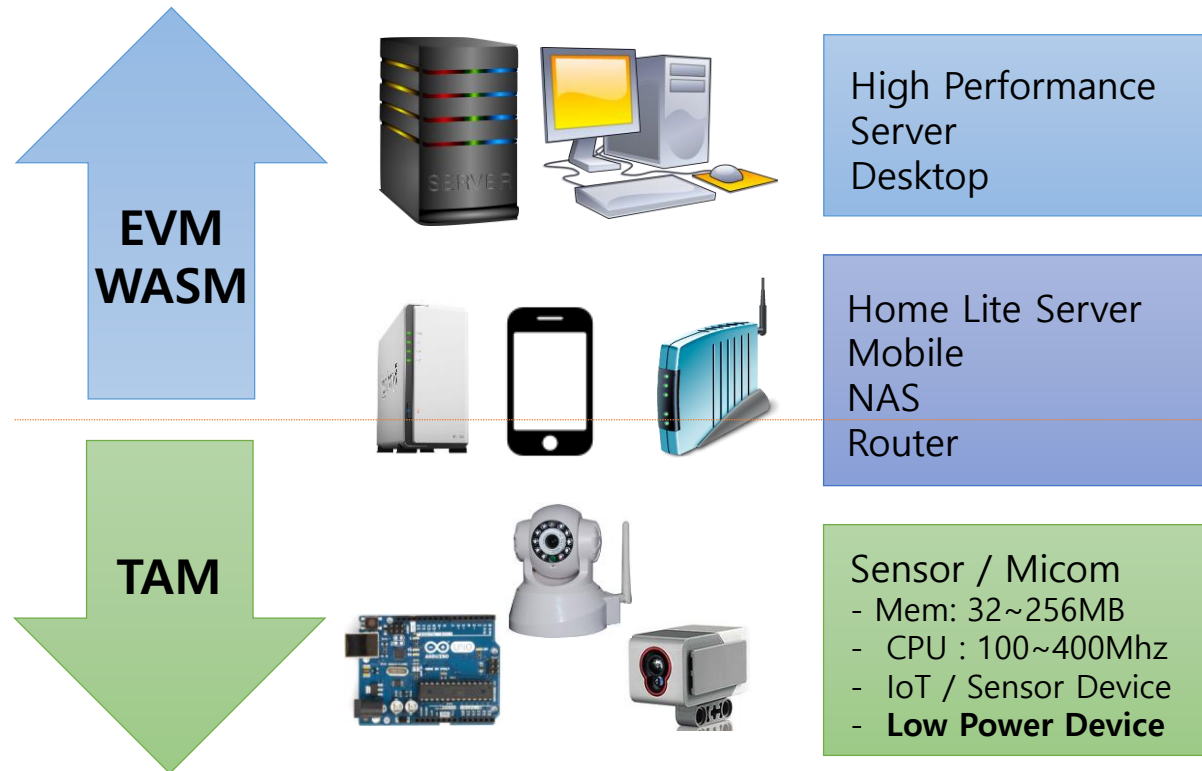
7. TAO's approach

- ▶ **Philosophy of TAO Chain Architecture.**
  - 1) DeCentralized Approach.
  - 2) All things has reason of existences.
  - 3) Each things has basic way of behavior.
  - 4) All things has its own lifecycle and lifetime.
- ★ **Above basic philosophy will applying to TAO Blockchain universe.**

- ▶ **On TAO Blockchain applied on real field.**
  - One kind of Blockchain can not efficiently handle all functions, and all the data in the chain does not have to exist permanently.
  - [TAO is proposed as a life cycle and lifetime of a block chain](#), and it aims at an efficient structure to solve scalability problems and reduce network traffic. – [Blockchain Router will do proxy layer of blockchain universe](#)
  - Each Blockchain tech has strong field and weak field. We will diverse traffics to each effective blockchains.
  - **Real CPU instruction based TAM (Trust Application Machine)** will be applied for **light-weight IoT and Sensor devices**. and,
  - iTAO very litechain for IoT devices will be applied.

8. Invent TAM – RISC V or OpenRISC

▶ **TAM (TAO TrustApplication Machine) adapt Real RISC CPU.**

- RISC-V (https://riscv.org) or OpenRISC (https://openrisc.io) is open RISC instruction set machine.
- It is implemented real cpu and several level of instruction architecture. (32Bits/64Bits)
- It is no License problem, for using public blockchains.
- Also There's Many SoC Vendors participating.
- Very Similar RISC Based embedded devices CPU core architecture instruction set [eg. MIPS , ARM-CortexM0, ..]

9. Contract Machine Resource Allocation Diagram.

EVM WASM ↑

TAM ↓

High Performance
Server
Desktop

Home Lite Server
Mobile
NAS
Router

Sensor / Micom
- Mem: 32~256MB
- CPU : 100~400Mhz
- IoT / Sensor Device
- **Low Power Device**

▶ **TAM (TAO TrustApplication Machine) is for Lite-weight IoT CPU.**
- SmartContract and iDAPP will be run on IoT Sensor device level of CPU.
- It needs elimated highly abstracted layer and very closed with industry using micom cpu instructions set.
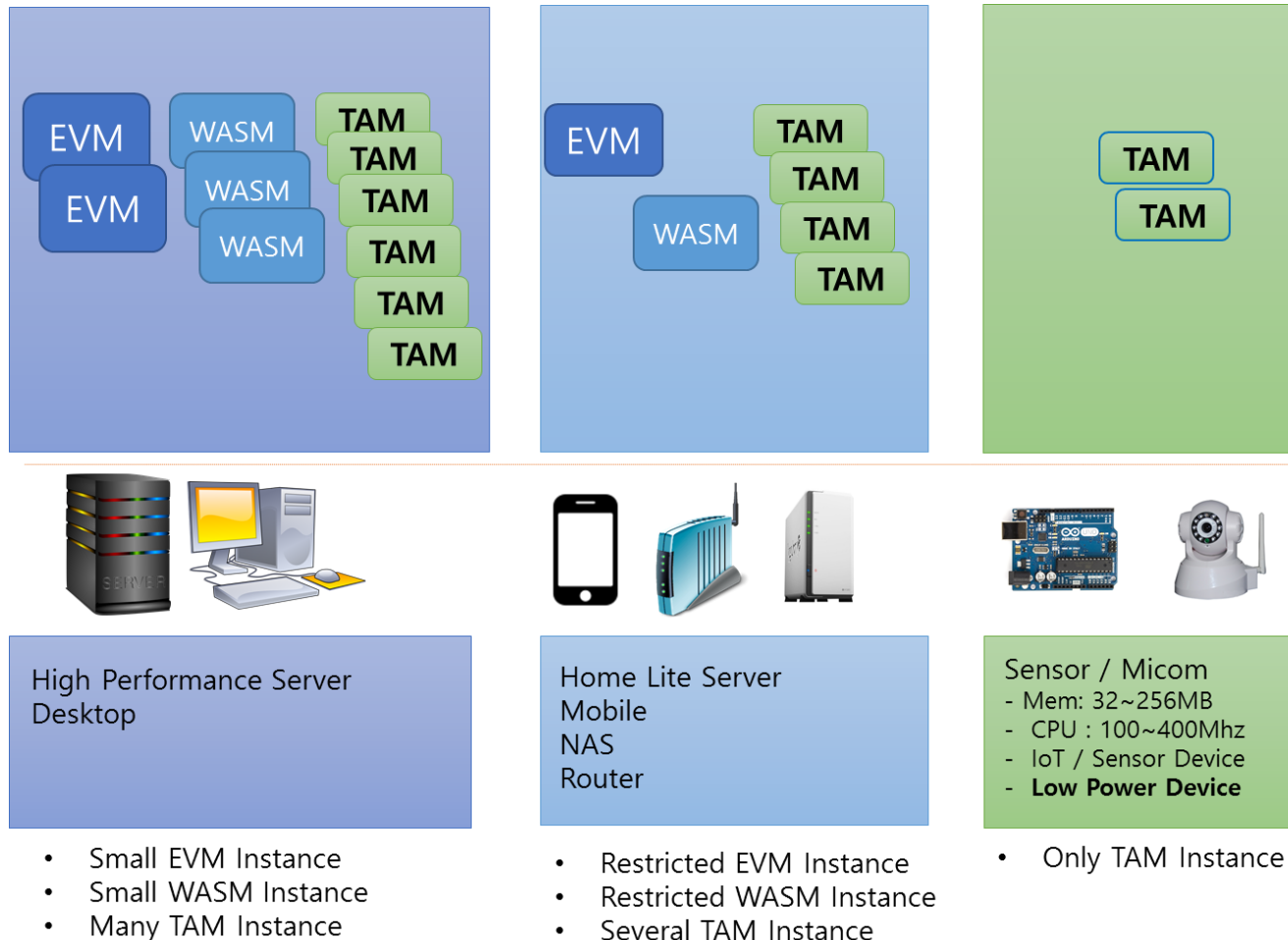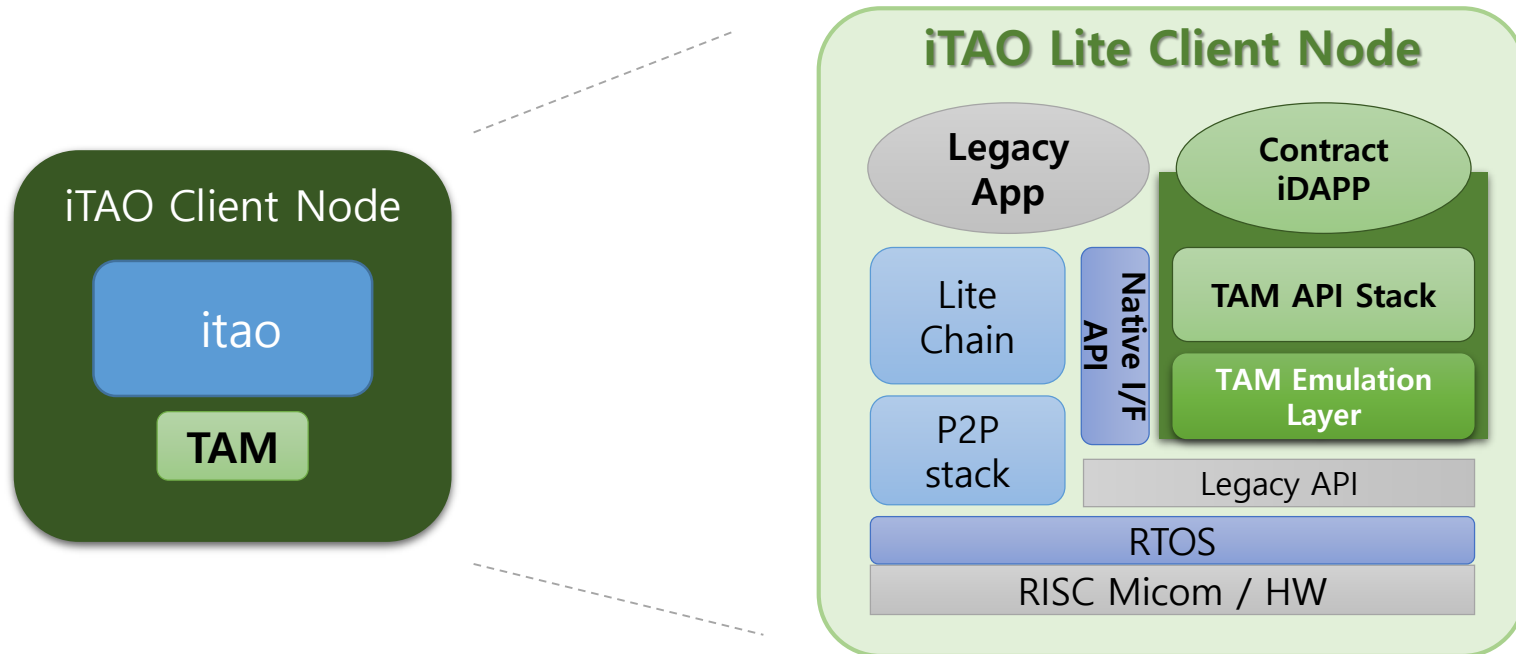
11. TAM on Client node , Lite Device diagram

▶ **TAM (TAO TrustApplication Machine) will implemented on IoT devices, with Lite emulation layers.**
- Client node, TAM will applied on TAM Emulation layer

iTAO Client Node

itao

TAM

iTAO Lite Client Node

Legacy App

Contract iDAPP

Lite Chain

Native I/F API

TAM API Stack

P2P stack

TAM Emulation Layer

Legacy API

RTOS

RISC Micom / HW

12. TAM on Full Client node diagram

▶ **TAM (TAO TrustApplication Machine) will implemented on IoT devices, with Lite emulation layers.**
  - Full Client node, TAM will applied on TAM VirtualMachine will be applied.
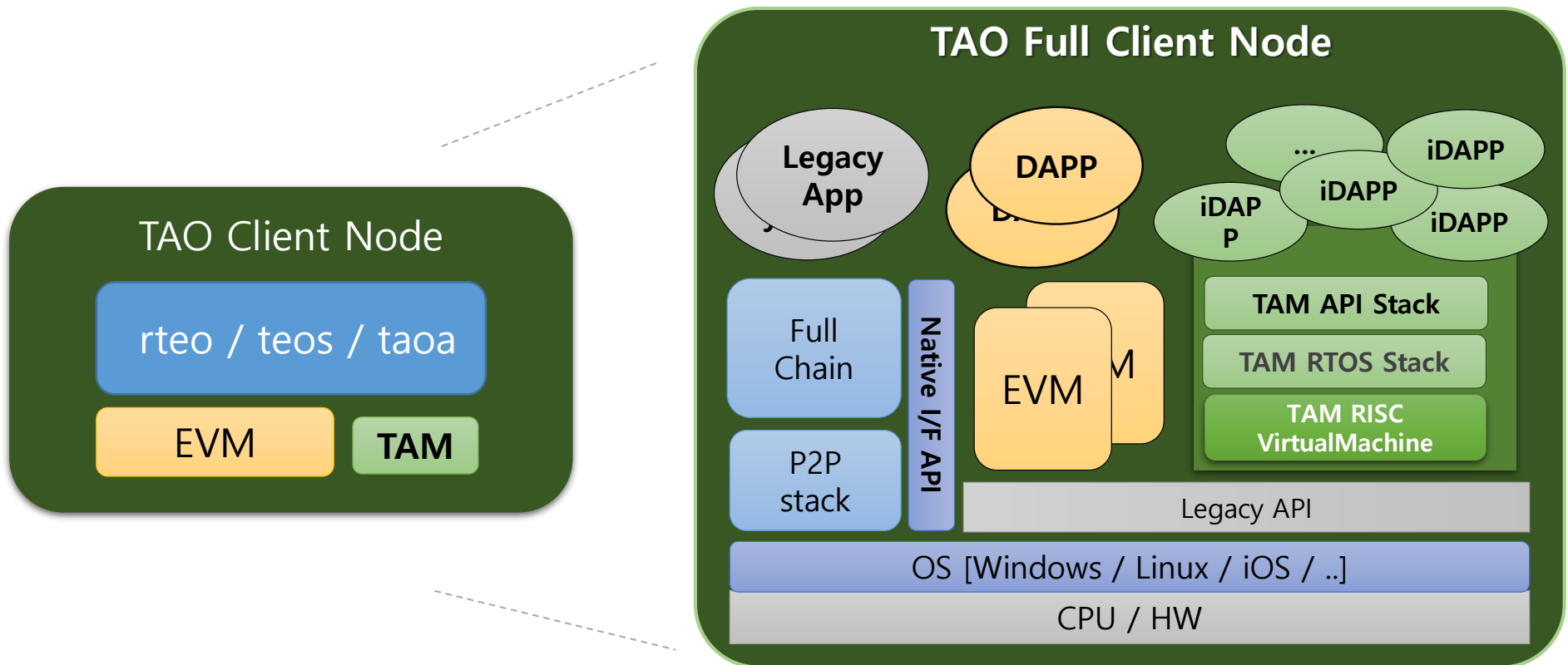
13. General DPOS chains efficiency and security issues.

- ▶ **DPOS – Efficiency and Security issues.**
  - POS/DPOS has very effective blockchain consensus algorithm.
  - It is very energy saving compared than PoW (Proof-of-Work) Bitcoin mining method.
  - Very Higher TPS(Transaction per Seconds) and Short Blocktime Compared than PoW Blockchain.
  - But, there's several persistent problem is exists. that's related to Blockchain Security issues.

★ Except of above : "The Rich get Richest, The Poor get Poorest" Serious.
  - Nothing at Stake, Stake grinding .. Validator node DDOS, and Validator insider hack.

14. TAO will solve following ways of DPOS security issues.

▶ **Min-Max node Funds capping, and GeoLocationally diversifying.**

- Consensus policy that sets the fund cap of **Hardcap / Softcap** to the verification node.

- If Funds will over max cap staking, Stake-rewards will limit, at given conditions.

- Minimum Funds staker should be participates on validators nodes.

- Geolocationally diversified of physical nodes, prevent of some regions' disaster of network down. or prevented from participating in the same network IDC segment.

- Ensure that **10% of geolocation and IDC network nodes in poor network area**s are included. This means equal opportunity, but also means that if the network situation is physically weak, DDOS itself can not easily attack the 10% node.

▶ **Expected Result and Reason.**

- Validator node diversifying.

- Weaken attack on validator nodes funds.

- provide Liquidity on exchange or real p2p trading on funds.

- Funds diversifying to more P2P accounts, it will make more value on funds. and increase activities on blockchain.

15. Overall TAO architecture.
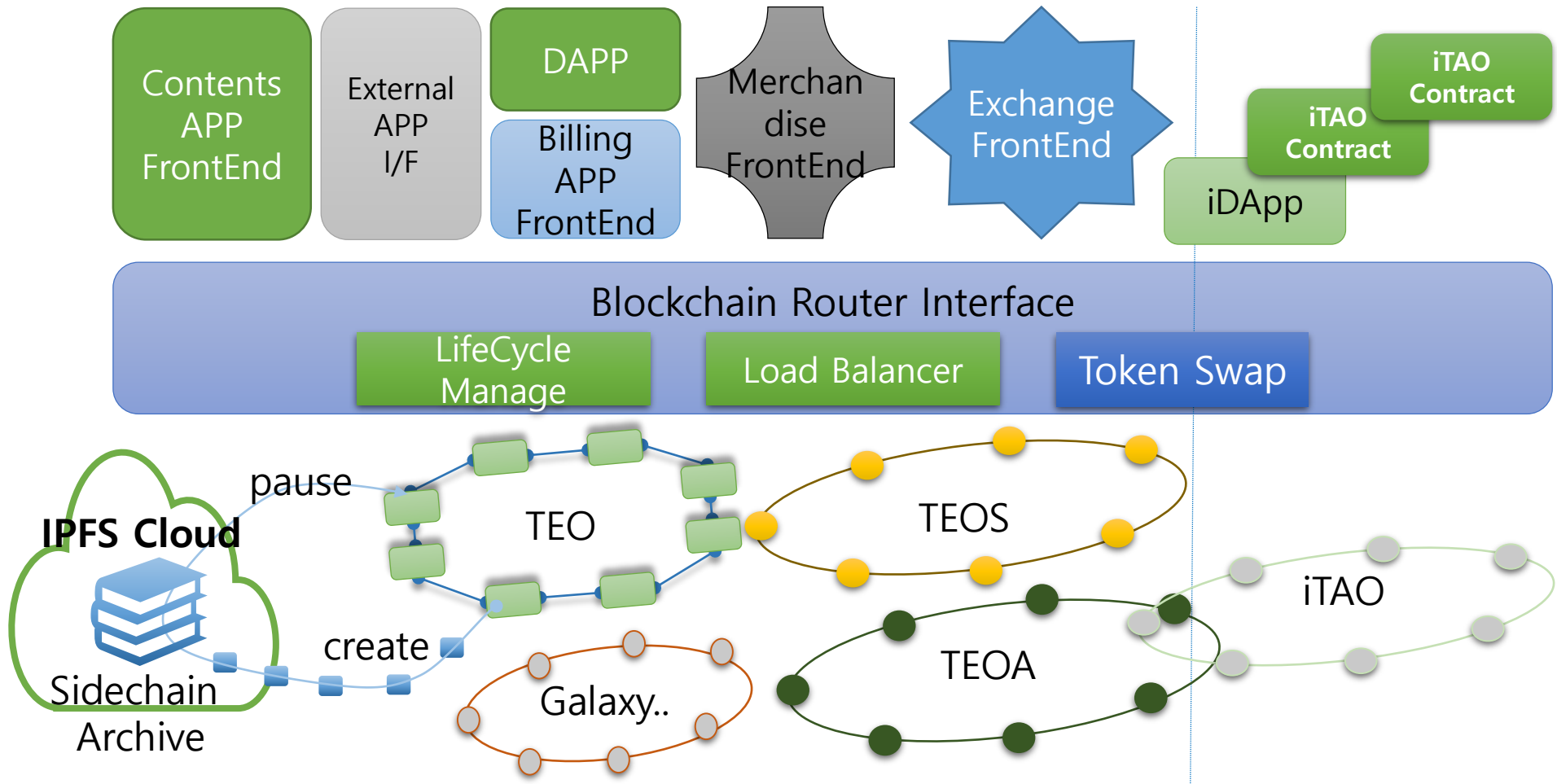
16. Apply SideChain fork for TAO architecture.

Original chain

Fork new-id of
EmptyChain
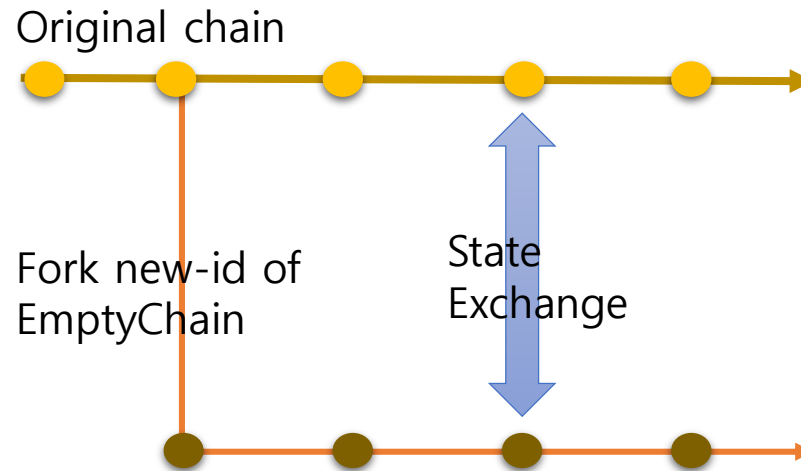
State
Exchange

▶ **Side-Chain will new Empty chain of parent chain.**
- Child Side-chain will inherit of parent chain, But, funds state will initialized with new chain-id.
- funds states will be state exchanged to side-chain.
- Side chain will be reach of end of lifecycle, side chain will be archived on P2P Network filesystem.
- Final sidechain states will merged to main chain.

Appendix

A-1. Advantage applying DeCentral System on IoE and AI?

more secure. more participants. more industry pie.

▶ **Privacy : Maximized.**
    Private Key and M2M Payment system will be blockchain based operated,
    Key is not stored and handled in central server. so, It is handled by IoE
    devices Owner , not manufacturer, no backdoor.
• It can do door-key/ car-renting shared by directly rentee and renter.

▶ **SmartContract utilities : More Secured Sharing and Control a Car**
    DAPP (DeCentralized Application) will do make possible contract.
    when the RentHouse/ RentCar is expired rent-duration.
• It can do police alarm , when car is hijacked or not returned.
    - It is can be programmed without privacy problem.

▶ **On DApp can make Marketplace : Buy and Sell Any features.**
    Any Feature Applying IoE and AI utilities made DAPP.
    Also, AI DeepLearning Infra will do Buy and Sell.
    DeepLearning Research Resource will do Buy and Sell.
• **Differencies are consumer/provider is all participants.**

A-2. AI MarketPlace.

▶ **Blockchain Based Resource Sharing platform**
  - AI Infra provider will sell their computing resource to Marketplaces.
  - Independent AI Researcher Group contributes research and output.
  - Each of Data Provider (Personal or Anywho) will contributes data.
  - Make AI based Service and Research final algorithm (Kernel or Pattern) will sold on Market places.
  - DApp will apply for DeepLearning researched output function operate on Blockchain, and it is buy and sold.

▶ **On AI Marketplace : Buy and Sell Any things on related AI.**
  Any Feature / Any Datum Applying for IoE and AI , It can be reward on it.
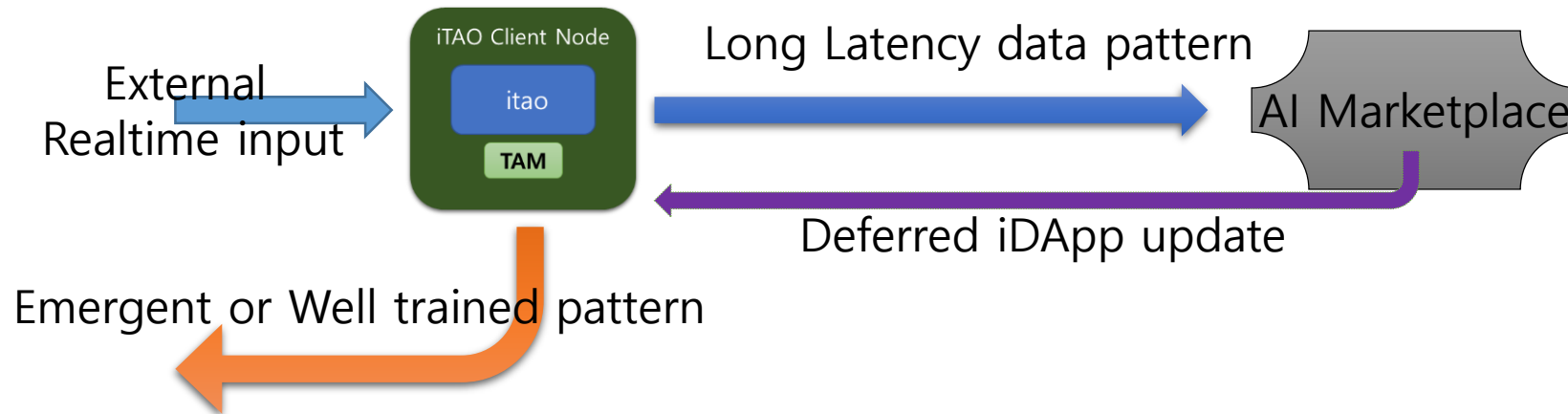 - **Differencies are consumer/provider is all participants.**

A-3. AI MarketPlace Diagram.
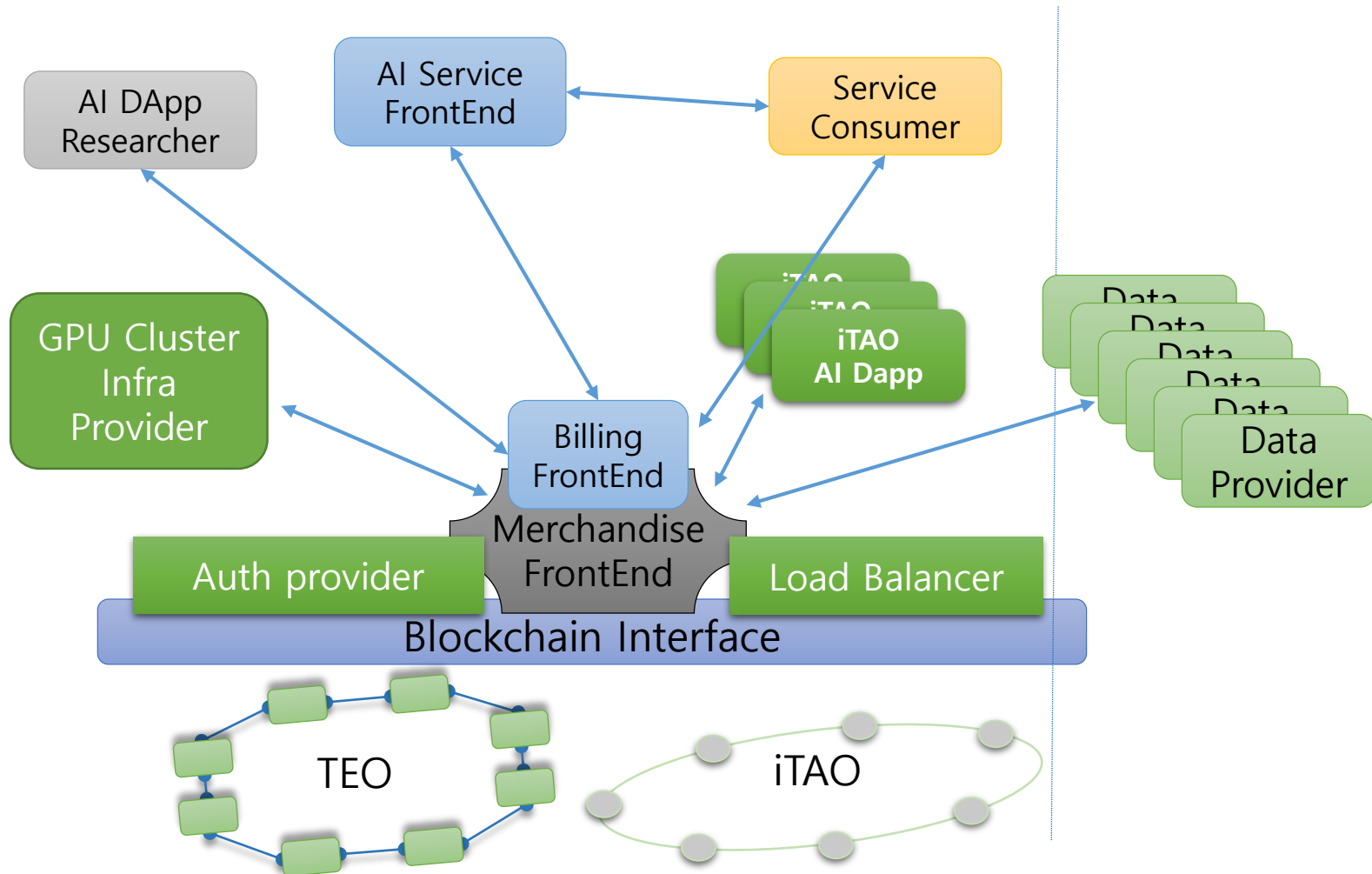
A-4. Applying DeepLearned Dominant pattern on IoE.

Well-known pattern of input, IoE devices react emergently. and feed to AI Marketplace.

iTAO Client Node

itao

TAM

External Realtime input

Long Latency data pattern

AI Marketplace

Deferred iDApp update

Emergent or Well trained pattern

▶ **Priority based Learning and Update patterns.**
- IoE Clients has well trained data pattern set, if Input is similar possibilities very high (eg. 90% accuracy) , fast return the output.
- In the same time, feed to AI Market places.
- Another Researched output will be back to IoE Clients, with iDAPP type.

End Of Documents
-Thank you-
-감사합니다-
-谢 谢-
- ありがとうございます-
-Mercy-
-Danke schön-