Web3 AI
Solutions & Possibilities

Heung-No Lee
Professor GIST/CEO LiberVance

Agenda

1. Short bio
2. Transformer and LLMs
3. Web3 AI
4. My AI Network

Short bio of HN Lee

Wireless Communications
PHD/MS/BS

HRL LABORATORIES

DARPA/Boeing/Raytheon/Hughes Projects
Wireless Ad Hoc Network, Fractal Internet Traffic Engineering

University of Pittsburgh

NSF, PDG, NIH Projects
MIMO Communications, Wireless Networks

GIST

NRF, ADD, AICA, IITP Projects
Information Theory, Blockchain, Machine Learning
Dean of Research: Gwangju AI Hub City of Korea

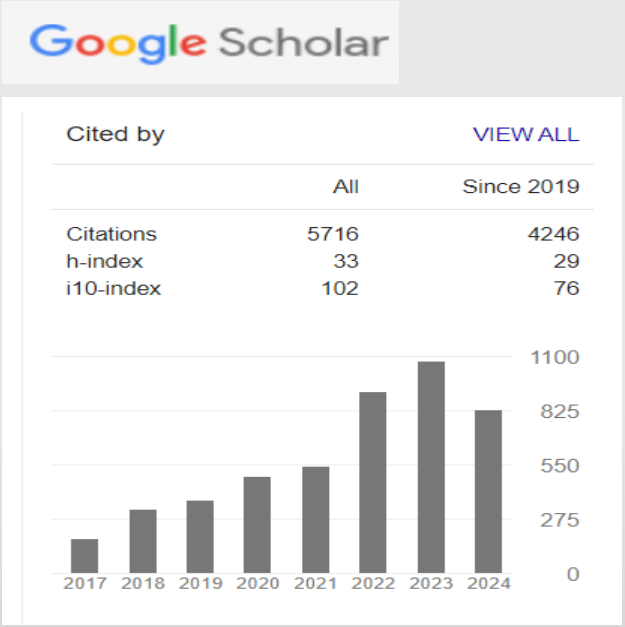
LiberVance

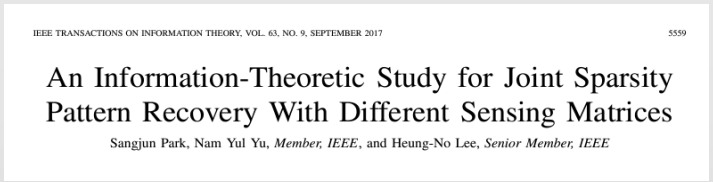
Scholarly Achievement

	Journals	Conf.	Patents Registered	R&D Funding
International SCI	**120+**	**99**	11 (USA)2 (Japan), 3 (PCT)	1.2 million USD
Korean	14	99	32 (Korea)	16 million USD
Sum	144+	198	48	17.2 million USD

Recent Patents Registered

발명의 명칭	Nation
스택 머신 프로그램을 위한 범용 영지식 스나크 증명 시스템 및 방법	USA
블록체인의 거래검증시스템, 및 블록체인의 거래검증방법	USA
블록체인 전자투표시스템, 그 시스템의 운용방법	USA
검표자가 필요 없는 영지식 증명과 스마트 컨트랙트 기반 블록체인 투표 시스템	USA
새로운 블록체인 및 암호화폐 작업증명 생성, 증명, 검증 시스템	USA




IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 63, NO. 9, SEPTEMBER 2017 5559

An Information-Theoretic Study for Joint Sparsity Pattern Recovery With Different Sensing Matrices

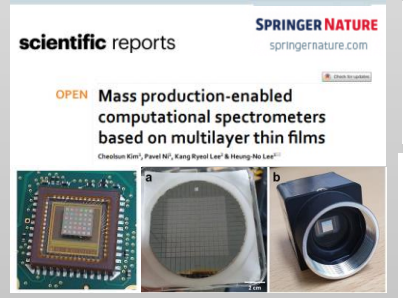
Sangjun Park, Nam Yul Yu, *Member, IEEE*, and Heung-No Lee, *Senior Member, IEEE*

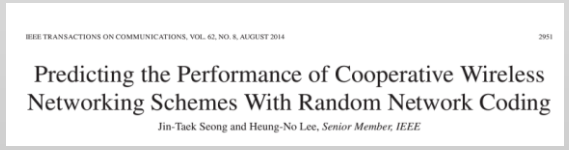

IEEE TRANSACTIONS ON SIGNAL PROCESSING, VOL. 66, NO. 12, JUNE 15, 2018 3311

Intentional Aliasing Method to Improve Sub-Nyquist Sampling System

Jehyuk Jang, Sanghun Im, and Heung-No Lee, *Senior Member, IEEE*

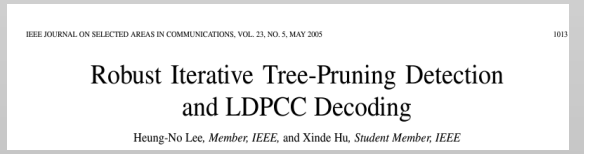
Categories	
Machine Learning, Signal Processing & Information Theory	80%
Blockchain & Cryptocurrency	20%




IEEE TRANSACTIONS ON COMMUNICATIONS, VOL. 62, NO. 8, AUGUST 2014 2951

Predicting the Performance of Cooperative Wireless Networking Schemes With Random Network Coding

Jin-Taek Seong and Heung-No Lee, *Senior Member, IEEE*


IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 23, NO. 5, MAY 2005 1013

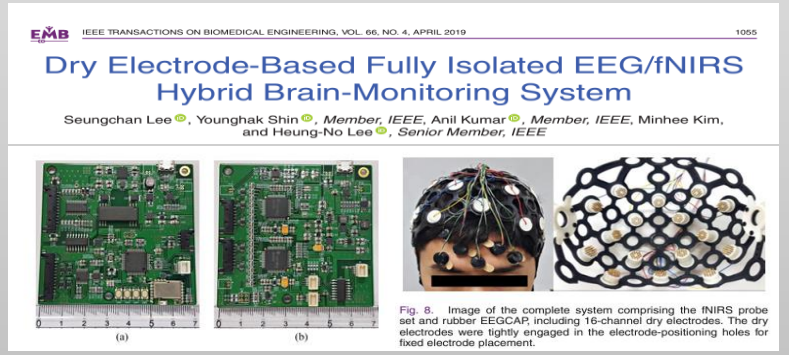
Robust Iterative Tree-Pruning Detection and LDPCC Decoding

Heung-No Lee, *Member, IEEE*, and Xinde Hu, *Student Member, IEEE*

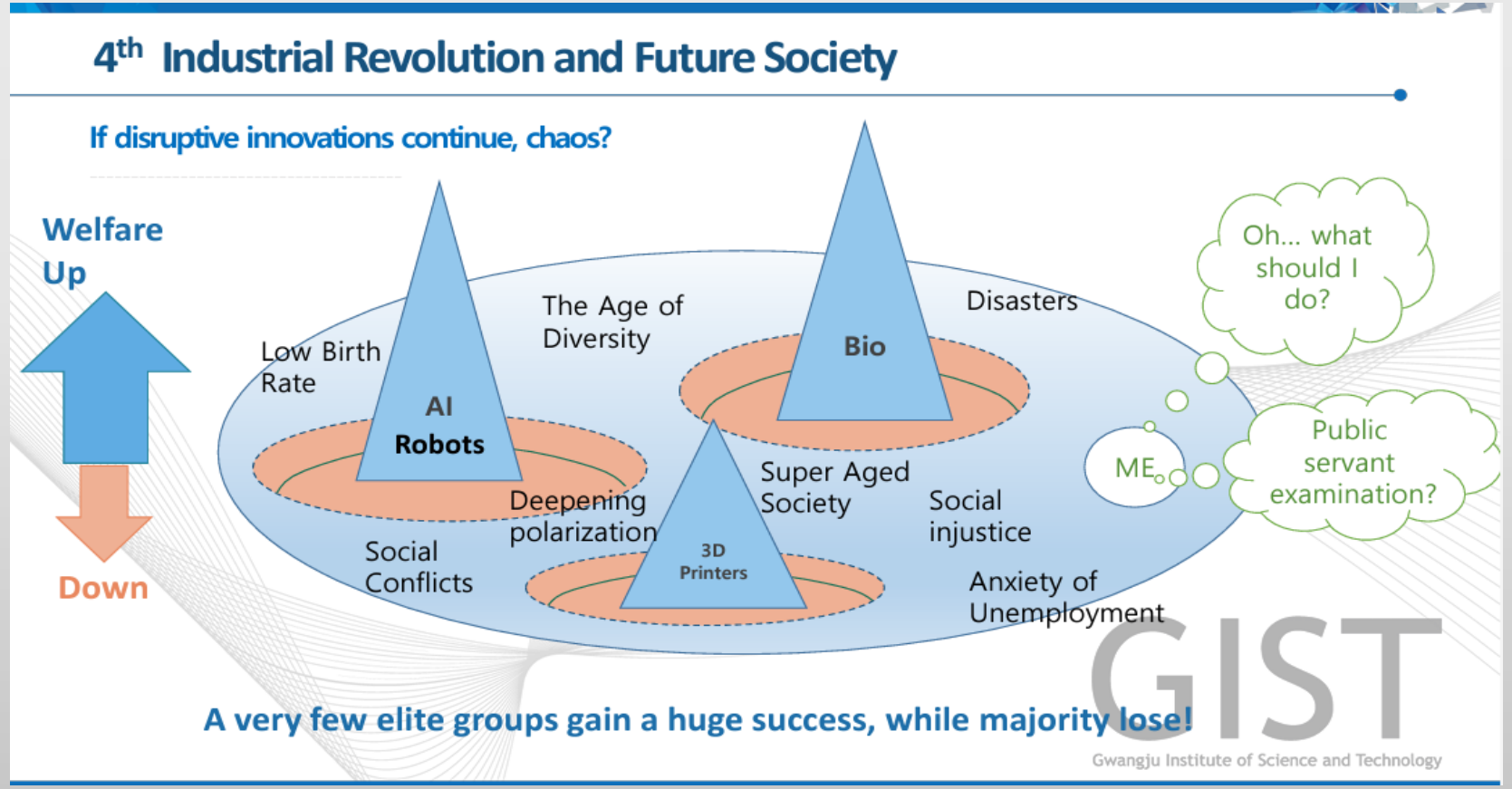

IEEE TRANSACTIONS ON ULTRASONICS, FERROELECTRICS, AND FREQUENCY CONTROL, VOL. 67, NO. 9, SEPTEMBER 2020 1785

High-Resolution Ultrasound Imaging Using Random Interference

Pavel Ni, *Student Member, IEEE*, and Heung-No Lee, *Senior Member, IEEE*



Why I got into blockchain & cryptocurrency?



Director of GIST Institute Heung-No Lee, The K-Hotel, Seoul, 7.14, 2017

Today, Gwangju is the AI hub of Korea, how?

Director of GIST Institute Heung-No Lee, The K-Hotel, Seoul, 7.14, 2017

Project gained traction under the name, AI Startup Town.
Location is the northern side of GIST campus!

Large Language Models

OS models are available to make AI assistants.

Open Source vs. Closed Source

- GPTs are not open source
- Transformer model is open source
- Meta's LLaMa models are open source
- LLaMa3.1 is as good as GPT4.

https://about.fb.com/news/2024/07/open-source-ai-is-the-path-forward/

Meta

Open Source AI Is the Path Forward

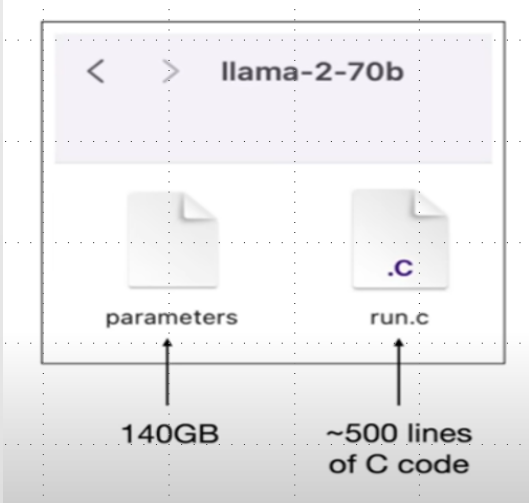
July 23, 2024
By Mark Zuckerberg, Founder and CEO

Why? People want to
- Have their own model
- Control their own destiny
- Protect their data

Good for Meta too?
- First mover advantage
- People build future on it

Model	Source Code	Training Data	Checkpoints
LLaMa 3	Open	Partially Open	Open
BLOOM	Open	Open	Open
Falcon 180B	Open	Not Open	Open
Flan-T	Open	Not Open	Open

LLaMa is a two file system.



80GB Memory

AMD EPYC 9334 듀얼 NVIDIA A100 80GB 2WAY 최대 8GPU GPU서버 AI 연구 학습 딥러닝 이중화 4U 랙타입

94,714,590원 **8 GPU**

8/24(토) 도착 예정

Small - hand phone
Medium - PC or Laptop
Large - Server
ULarge - Cluster

Llama Models

Model	Launch date	Model sizes	Context Length
Llama 2	7/18/2023	7B, 13B, 70B	4K
Llama 3	4/18/2024	8B, 70B	8K
Llama 3.1	7/23/2024	8B, 70B, 405B	128K

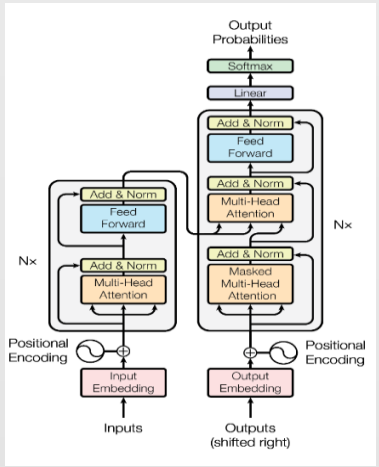
GPT3.5 175B
GPT4.0 1T?

Transformer is a next word prediction model.

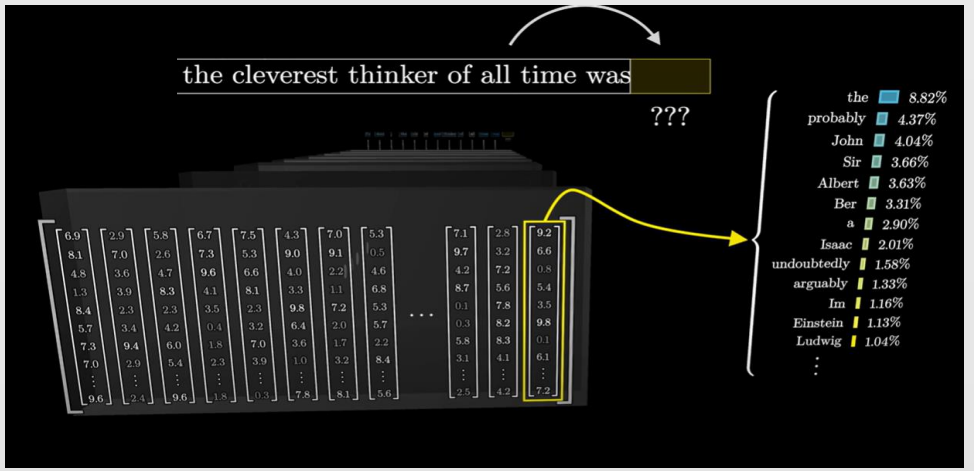
Input

the cleverest thinker of all time was MASK

X



Context length = 8

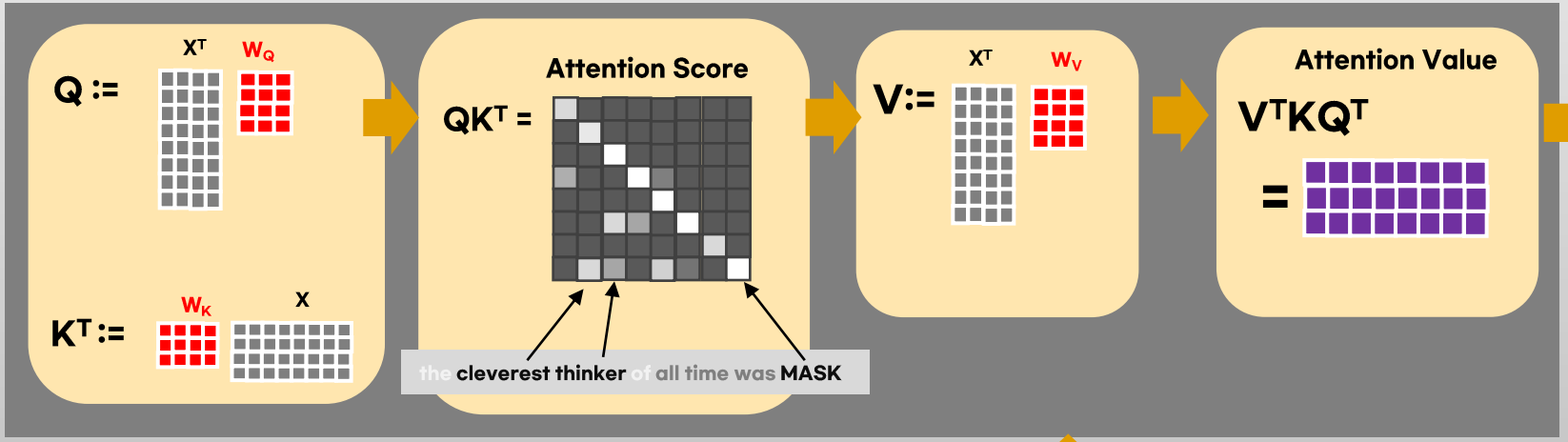


Output

"the"

But, unmask reveals

"Einstein"



"the, Einstein"

Compute Loss

Back propagation

Parameter matrices W_Q, W_K, W_V are updated

How does it work?

We know
- How to iteratively adjust billions of parameters and make it better at predicting the next word

We don't know
- How these parameters work together achieving it

It builds and maintains a knowledge database, but it is imperfect.

- "Reversal Curse" example
- Q: Who is Tom Cruise's mother?
- A: Mary Lee Pfeiffer (correct)

- Q: Who is Mary Lee Pfeiffer's son?
- A: I don't know.

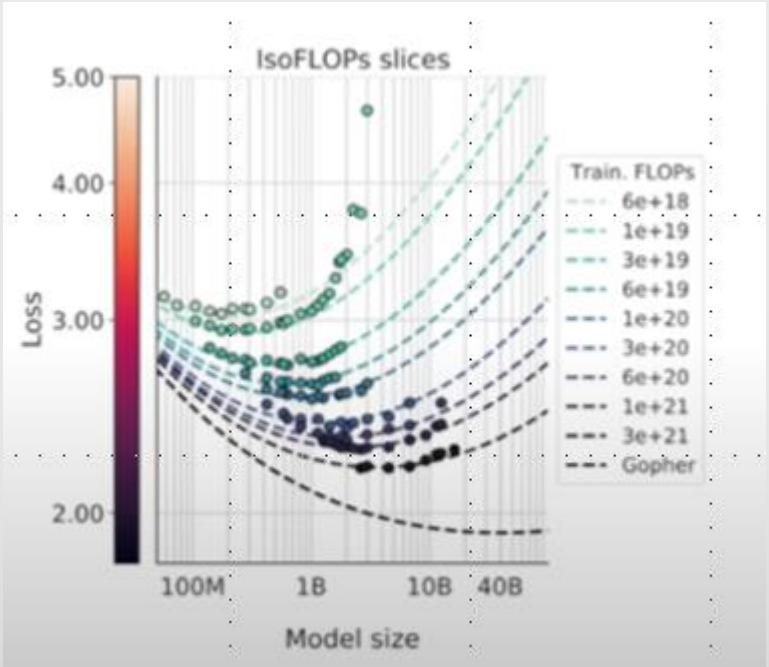
Aware that LLM outputs are probable artifacts!
- Need to develop sophisticated method to verify and correct them!

Retrieval Augmented Generation

We can expect better intelligence by scaling!

LLM Scaling Laws:

- Parameter Scaling: Larger models with more parameters tend to perform better.
- Data Scaling: Models trained on more data show improved performance.

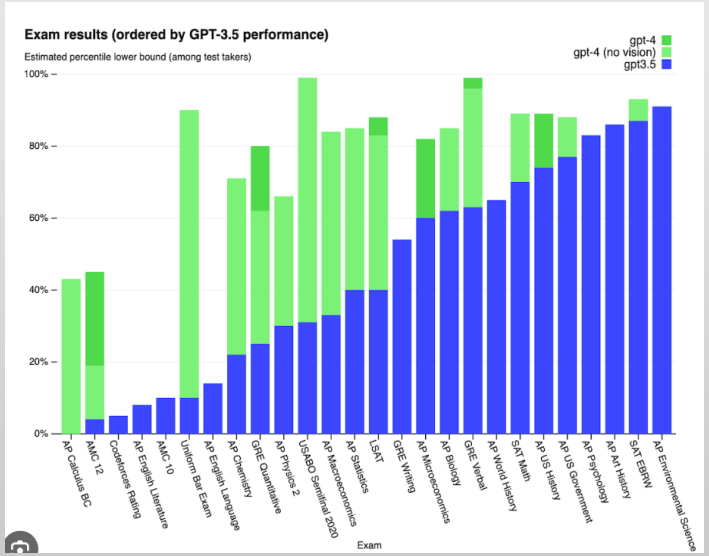


GPT3.5 175 billion parameters

GPT4.0 possibly 1 trillion parameters

Emergent Abilities

- Few shot
- Zero shot



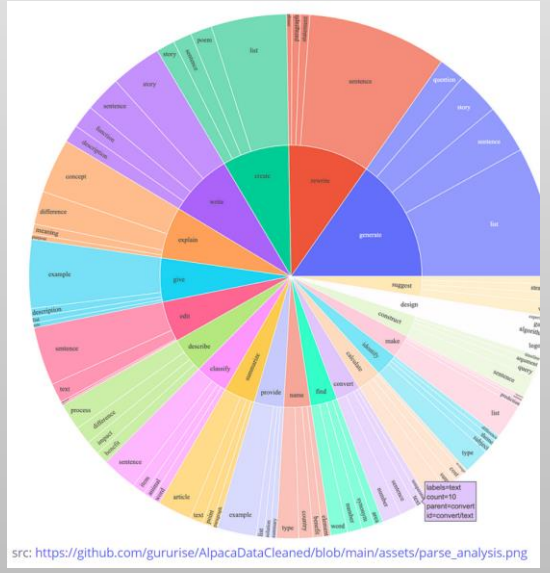
Two types of training

Pre-training (once/year)
- Collect 10 TB of text
- Get a cluster of 10,000 GPUs
- Feed the text into LLM ($2M, month)
- Obtain the pre-trained (PT) model

Next word prediction enables the LLM to learn a lot about the world!

Fine-tuning (once/month)
- Consult Alpaca paper for instructions
- Get a single GPU or GPU server.
- Generate 100K high quality Q&A responses (or buy)
- Fine-tune the PT model on Q&A responses (1 day)
- Obtain FT model

Makes an assistant


src: https://github.com/gururise/AlpacaDataCleaned/blob/main/assets/parse_analysis.png

Create
Summarize
Rewrite
Suggest
Describe
Edit
Classify
...

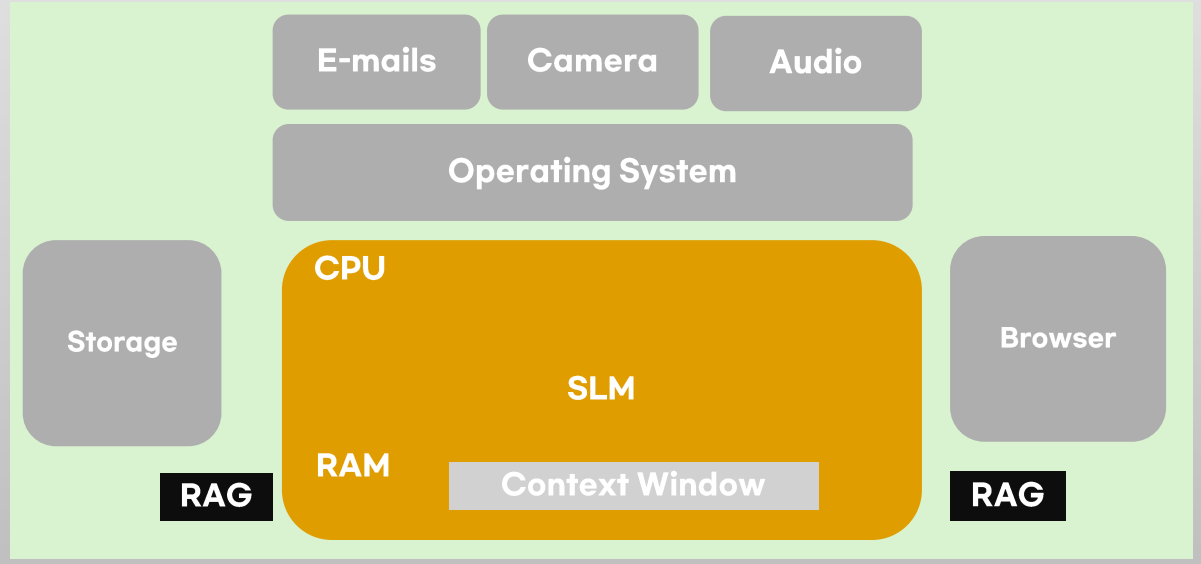
AI assistant in laptops & mobile phones

Apple Intelligence

Apple Intelligence is the personal intelligence system that puts powerful generative models right at the core of your iPhone, iPad, and Mac and powers incredible new features to help users communicate, work, and express themselves. You can bring these Apple Intelligence features right into your apps.

An AI agent is an AI assistant which autonomously performs tasks for me.
It listens to me or watch my screen activities and assists me:

- Make travel plan
- Write a report
- Carry out on-line research

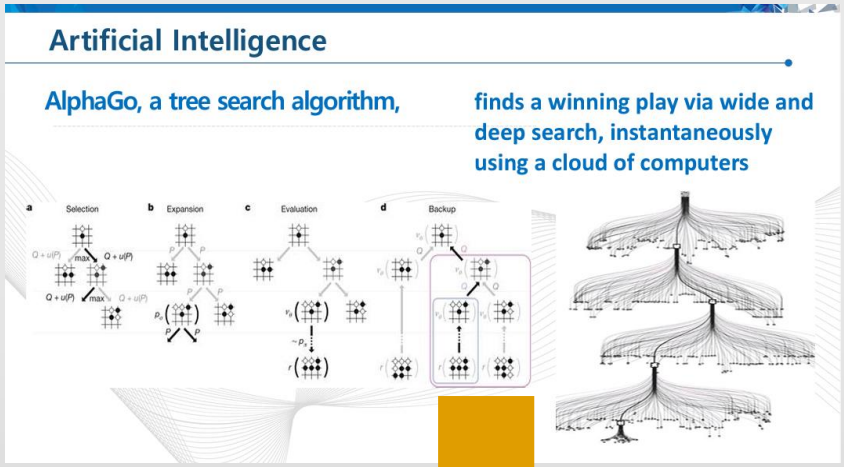


You can run your SLM on device.
But for medium and large models,
you have to choose between

Web2 and Web3

Two types of AI advances, and future

Broad and Deep Search



Generative AIs

A network of AI agents

- Each node is a domain expert
- Local self-learning
- Global cooperative learning network
- Solving real-world problems
- Evolution of network intelligence

Web3 AI

Web2 vs Web3

Web 2 platforms:
Facebook, YouTube, Twitter, and Wikipedia.

They often control content distribution, data collection, and monetization, which are key aspects that Web3 seeks to decentralize and democratize.

Web3 infrastructure
- dApps
- NFTs
- DAOs
- Permissionless blockchains
- Users control their data and identity

Read **Read&Write** **Read,Write & Own**

Web3

Web3 represents the 3rd phase of the internet, focusing on decentralization, user control, and blockchain integration.

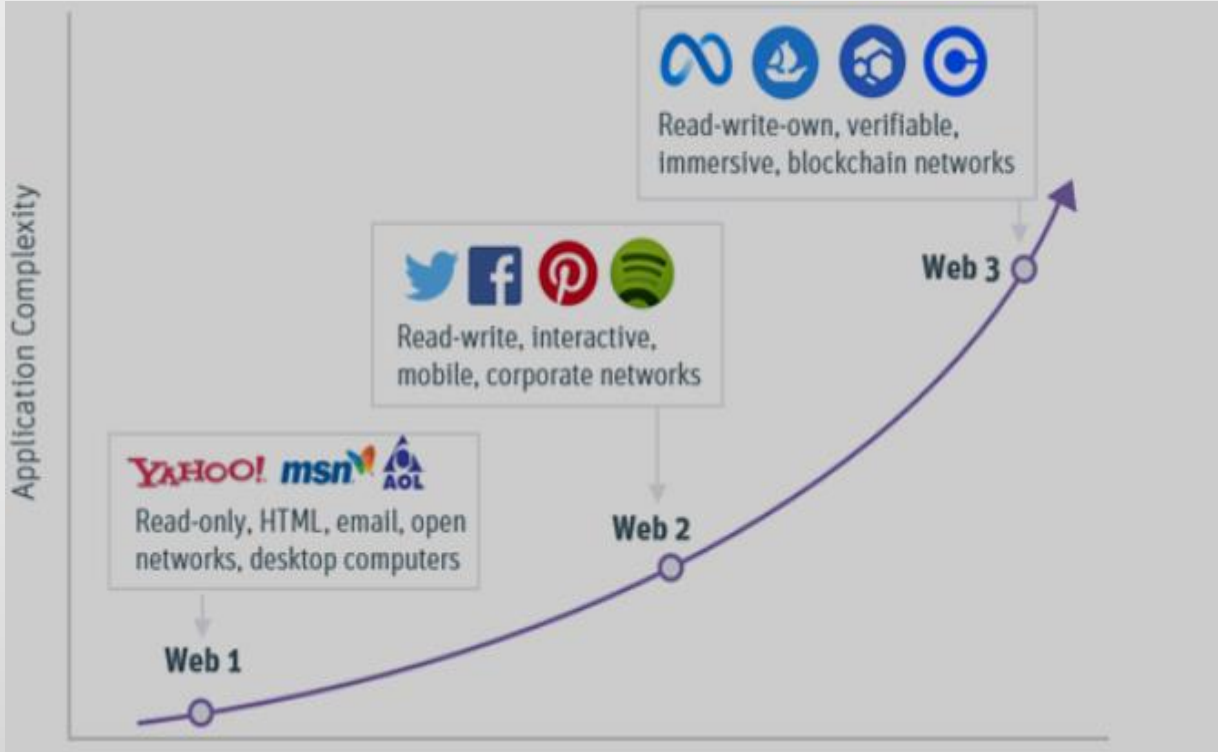
Origin:

- The term "Web3" was popularized by Gavin Wood, co-founder of Ethereum, around 2014.
- He envisioned a user-centric internet where applications would not rely on a central authority, and data would be owned by users.

Key Players:

- Gavin Wood (Polkadot), Vitalik Buterin (Ethereum), and companies like ConsenSys, Chainlink, and Protocol Labs.

Web3



Impact: Web3 could democratize the internet by enabling peer-to-peer transactions, reducing reliance on intermediaries, and creating new economic models based on tokens and decentralized governance.

Challenges:

- Scalability: Many blockchain networks face limitations in transaction speed and capacity.
- User Experience: Web3 applications are often less user-friendly than their Web2 counterparts.
- Interoperability: Connecting different blockchains and ensuring they work together smoothly is still a work in progress.

Overall, Web3 is rapidly evolving but still in its early stages.

The next few years will be critical in determining how widespread and impactful it becomes.

Web3 AI

Web3 AI refers to the fusion of Web3 with AI.

- The idea of Web3 AI is emerging.
- There are two types available today:
- (Type 1) Web3 AI aims to run and train AI models on decentralized, transparent, and permissionless Web3 infra such as blockchains, smart contracts, and tokens. For this, we need to create new systems where users can retain ownership of their data and AI models, benefit economically from AI models, and ensure privacy.
- (Type 2) This fusion allows AI to operate on decentralized platforms, enabling applications like decentralized autonomous organizations (DAOs) to utilize AI for governance, decision-making, and operations without relying on centralized entities.

Web3 AI

Prospect

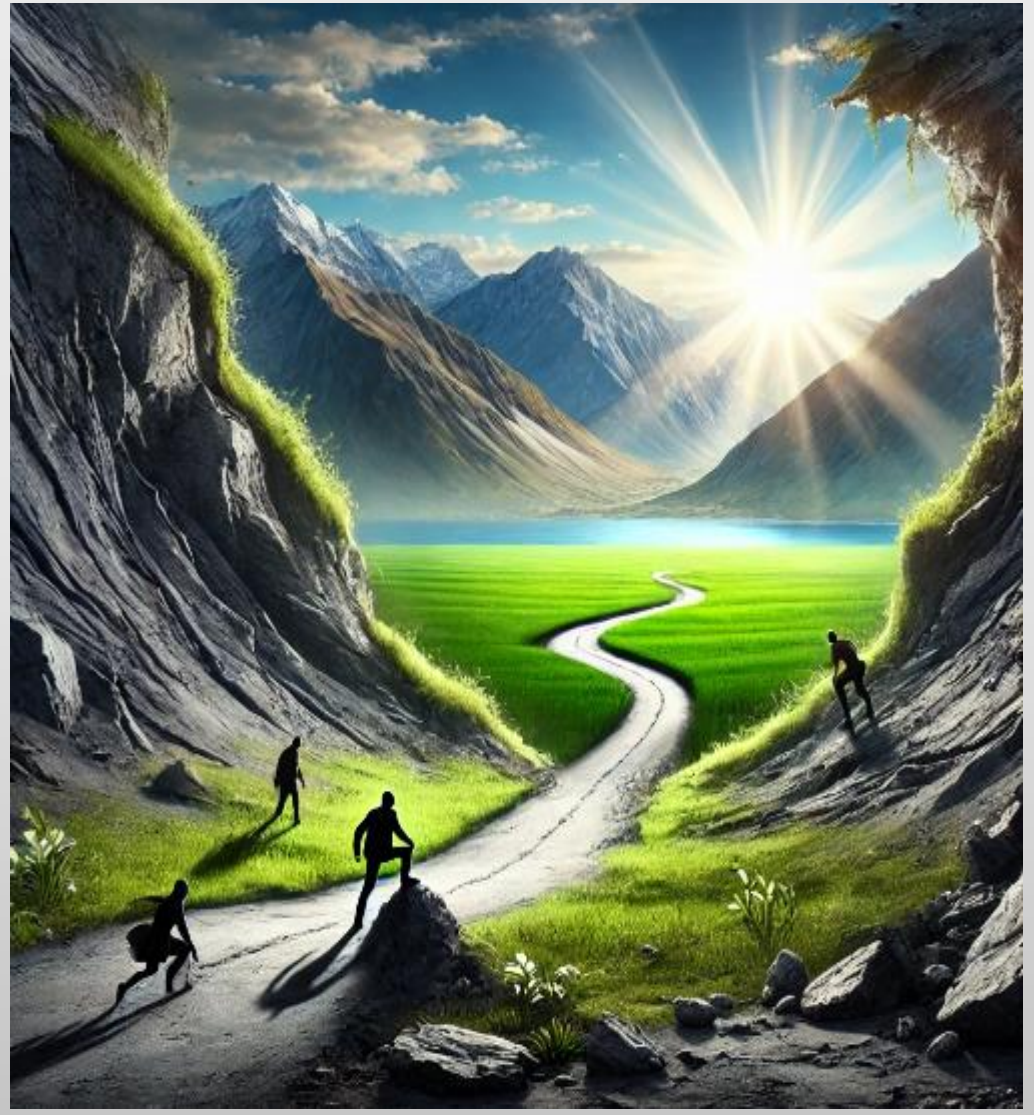
- The near-term prospects for Web3 AI are promising but also challenging.
- The integration of AI into Web3 platforms could disrupt various industries, including finance, healthcare, and content creation.

Challenges

- Scalability of blockchain technologies
- Need for decentralized AI models

Key Takeaways

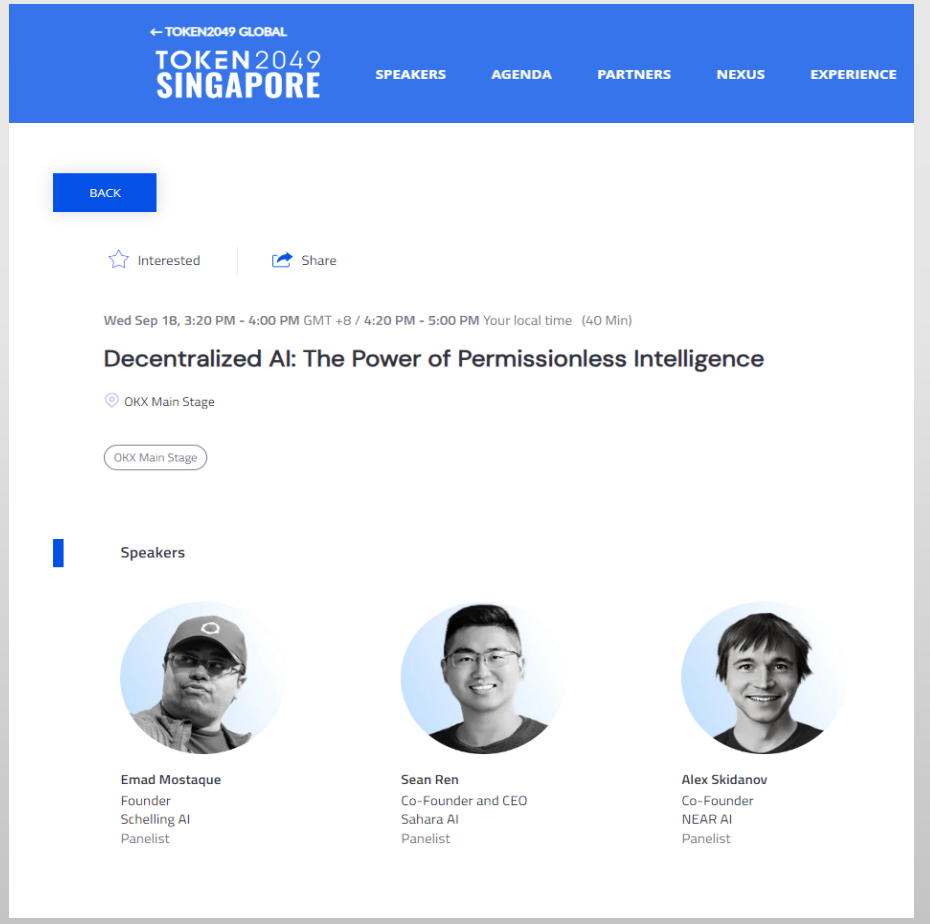
- Use not only ZKML, OPML, Federated Learning…
- But also layer-2 chains, sidechains, and off-chain computations/storages for a greater scalability.
- Allow people monetize their AIs
- Track AI transactions and get paid direct
- Encourage more cooperation among AIs
- Enable solving complex real world problems
- Empower people at the edge



Web3 AIs in Consensus 2024

1. AKASH Network: Tokenized decentralized GPU Network
2. Morpheus: Open Source Decentralized AI Network
3. GAIANET: Decentralized GenAI Agents Network
4. Oraichain: Multichain and off-chain AI compute
5. SingularityNET
4. Rise of the Machine Economy

Many more projects exist in the direction of Web3 AI.
➔ Will discuss this in My AI Network (competitive landscape)



DUBAI AI & WEB3 FESTIVAL

My AI Network

A global platform enabling **users to create, own, and monetize their AI agents** while ensuring data privacy

LiberVance

Vision

My AI era is coming.

Human Teacher

AI Teacher

Human Lawyer

AI Lawyer

Human Doctor

AI Doctor

Pain Points

Web2 AI monopolizes profits with data from people around world.

Not open source!

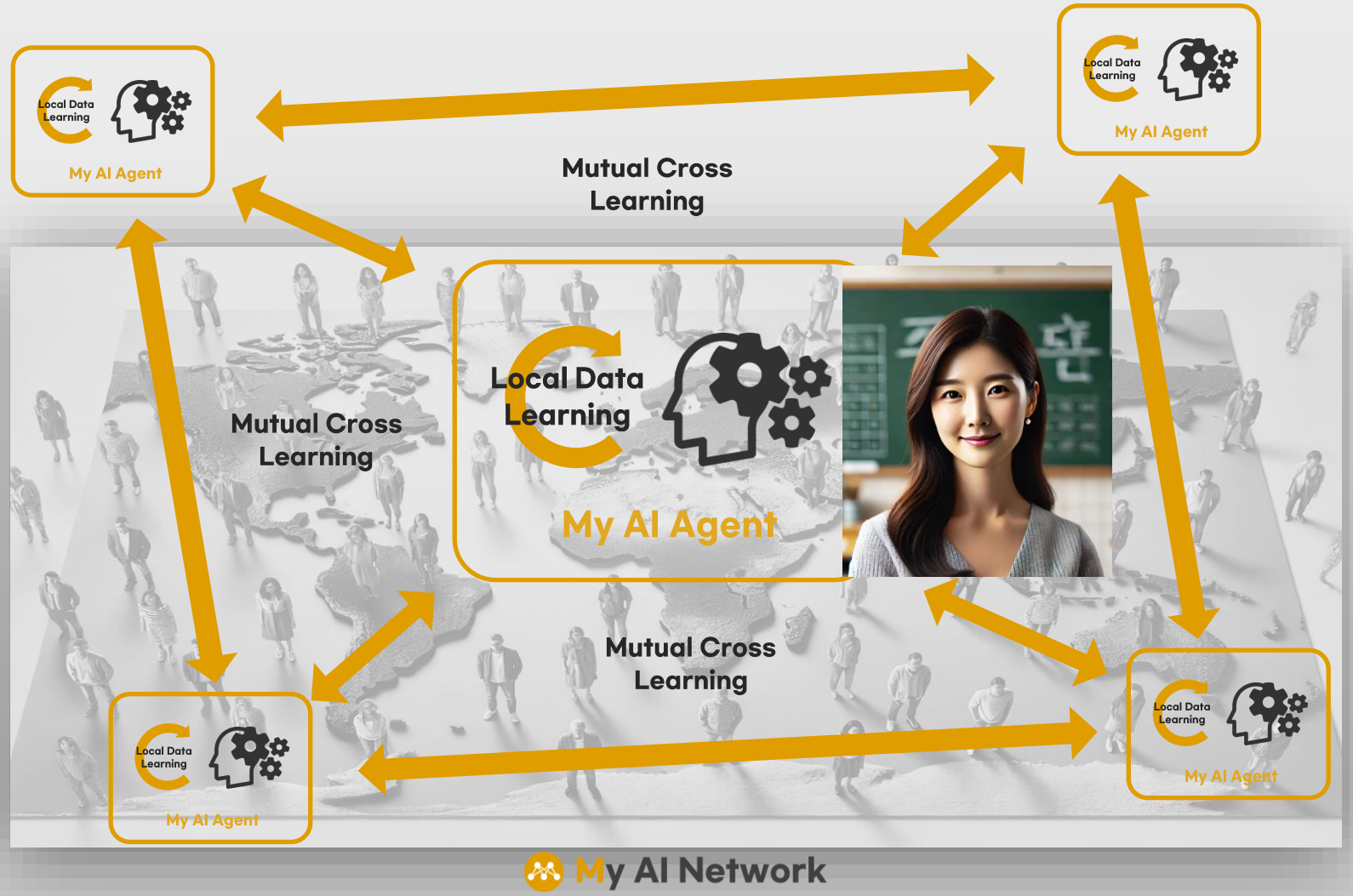
GDPR violation!

Web2 AI

Not verifiable!

Locked in closed ecosystem!

Our solution: My AI Network



It's a nexus of AI agents which co-evolves as a network intelligence via both continual local learning and mutual conversational learning!

Our Solution

Key Features of My AI Network

1 Drop & run agents : Allow anyone to create My AI agent with no coding!

- Install the 'My AI Train Tool' on your PC
- Just 'Drop' your own data to create and run your own My AI agent

2 Have them cooperate and grow smarter!

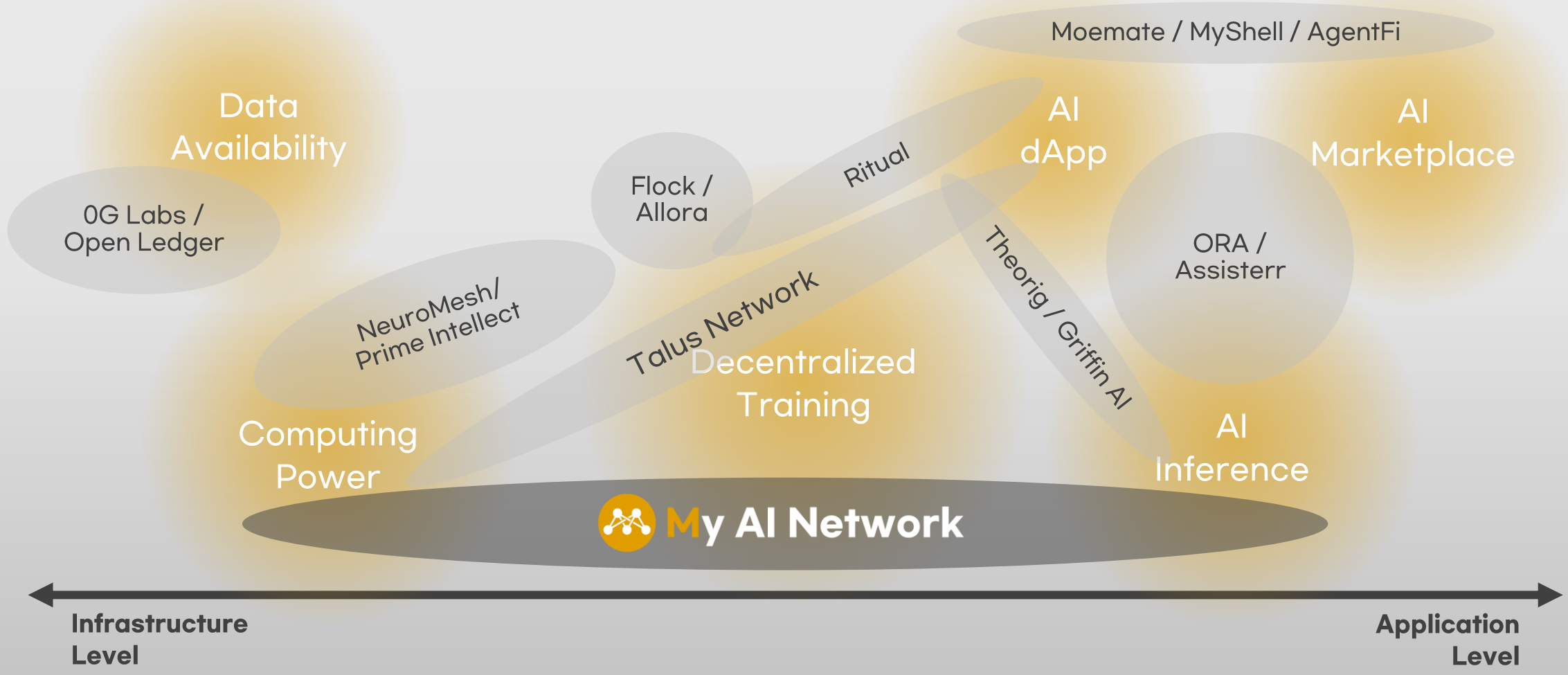
- On our platform, your My AI Agent grows smarter by interacting with other people's My AI agents

3 Verifiable AI Compute Cloud : Have a unique protocol stack!

- It is built based on open source modular AI Compute Protocol
- Primitives include PQS Cryptography / ECCVCC / PT Model / FT-RAG / ZKP / Web3

Competitive Landscape

We aim to position and focus on computing power, AI training & inference!



LiberVance

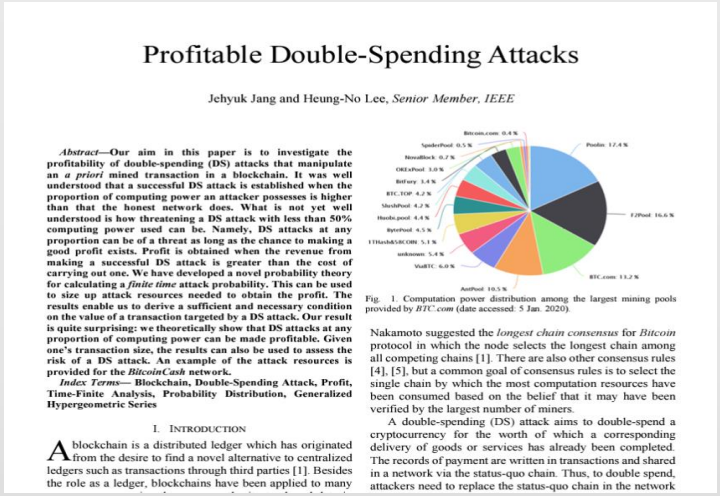
Unique Tech Stack

Our protocol primitives have been published in top scientific journals.

Implication

- Have expertise in AI agents
- Novel AI compute module
- Has been testing networks extensively

We are ready for My AI Network!



Profitable Double-Spending Attacks

Jehyuk Jang and Heung-No Lee, *Senior Member, IEEE*

***Abstract*—Our aim in this paper is to investigate the profitability of double-spending (DS) attacks that manipulate an *a priori* mined transaction in a blockchain. It was well understood that a successful DS attack is established when the proportion of computing power an attacker possesses is higher than that the honest network does. What is not yet well understood is how threatening a DS attack with less than 50% computing power used can be. Namely, DS attacks at any proportion can be of a threat as long as the chance to making a good profit exists. Profit is obtained when the revenue from making a successful DS attack is greater than the cost of carrying out one. We have developed a novel probability theory for calculating a *finite time* attack probability. This can be used to size up attack resources needed to obtain the profit. The results enable us to derive a sufficient and necessary condition on the value of a transaction targeted by a DS attack. Our result is quite surprising: we theoretically show that DS attacks at any proportion of computing power can be made profitable. Given one's transaction size, the results can also be used to assess the risk of a DS attack. An example of the attack resources is provided for the *BitcoinCash* network.**

***Index Terms*— Blockchain, Double-Spending Attack, Profit, Time-Finite Analysis, Probability Distribution, Generalized Hypergeometric Series**

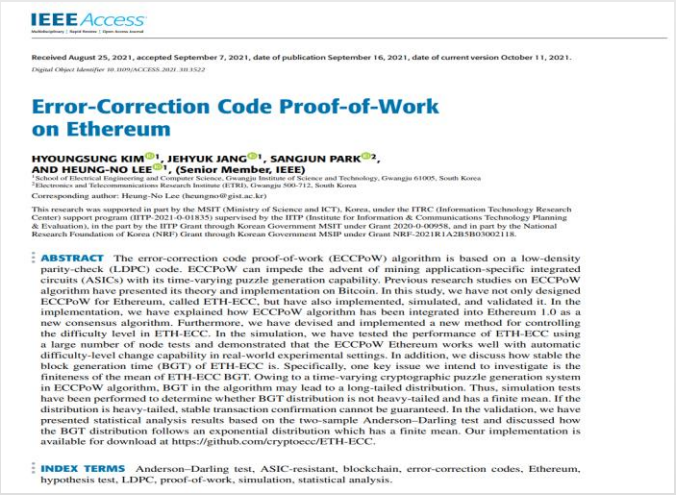
I. Introduction

A blockchain is a distributed ledger which has originated from the desire to find a novel alternative to centralized ledgers such as transactions through third parties [1]. Besides the role as a ledger, blockchains have been applied to many

Fig. 1. Computation power distribution among the largest mining pools provided by *BTC.com* (date accessed: 5 Jan. 2020).

Nakamoto suggested the *longest chain consensus* for *Bitcoin* protocol in which the node selects the longest chain among all competing chains [1]. There are also other consensus rules [4], [5], but a common goal of consensus rules is to select the single chain by which the most computation resources have been consumed based on the belief that it may have been verified by the largest number of miners.

A double-spending (DS) attack aims to double-spend a cryptocurrency for the worth of which a corresponding delivery of goods or services has already been completed. The records of payment are written in transactions and shared in a network via the status-quo chain. Thus, to double spend, attackers need to replace the status-quo chain in the network



IEEE Access

Received August 25, 2021, accepted September 7, 2021, date of publication September 16, 2021, date of current version October 11, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3113522

Error-Correction Code Proof-of-Work on Ethereum

HYOUNGSUNG KIM, JEHYUK JANG, SANGJUN PARK, AND HEUNG-NO LEE, (Senior Member, IEEE)

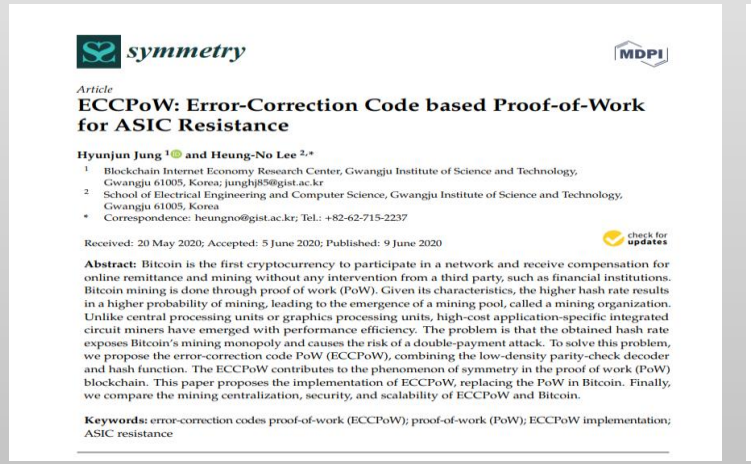
School of Electrical Engineering and Computer Science, Gwangju Institute of Science and Technology, Gwangju 61005, South Korea
Electronics and Telecommunications Research Institute (ETRI), Gwangju 500-712, South Korea

Corresponding author: Heung-No Lee (heungno@gist.ac.kr)

This research was supported in part by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (ITP-2021-0-01835) supervised by the ITP (Institute for Information & Communications Technology Planning & Evaluation), in the part by the ITP Grant through Korean Government MSIT under Grant 2020-0-00958, and in part by the National Research Foundation of Korea (NRF) Grant through Korean Government MSIP under Grant NRF-2021R1A2B5B03002118.

ABSTRACT The error-correction code proof-of-work (ECCPoW) algorithm is based on a low-density parity-check (LDPC) code. ECCPoW can impede the advent of mining application-specific integrated circuits (ASICs) with its time-varying puzzle generation capability. Previous research studies on ECCPoW algorithm have presented its theory and implementation on Bitcoin. In this study, we have not only designed ECCPoW for Ethereum, called ETH-ECC, but have also implemented, simulated, and validated it. In the implementation, we have explained how ECCPoW algorithm has been integrated into Ethereum 1.0 as a new consensus algorithm. Furthermore, we have devised and implemented a new method for controlling the difficulty level in ETH-ECC. In the simulation, we have tested the performance of ETH-ECC using a large number of node tests and demonstrated that the ECCPoW Ethereum works well with automatic difficulty-level change capability in real-world experimental settings. In addition, we discuss how stable the block generation time (BGT) of ETH-ECC is. Specifically, one key issue we intend to investigate is the finiteness of the mean of ETH-ECC BGT. Owing to a time-varying cryptographic puzzle generation system in ECCPoW algorithm, BGT in the algorithm may lead to a long-tailed distribution. Thus, simulation tests have been performed to determine whether BGT distribution is not heavy-tailed and has a finite mean. If the distribution is heavy-tailed, stable transaction confirmation cannot be guaranteed. In the validation, we have presented statistical analysis results based on the two-sample Anderson–Darling test and discussed how the BGT distribution follows an exponential distribution which has a finite mean. Our implementation is available for download at https://github.com/cryptoecc/ETH-ECC.

INDEX TERMS Anderson–Darling test, ASIC-resistant, blockchain, error-correction codes, Ethereum, hypothesis test, LDPC, proof-of-work, simulation, statistical analysis.



symmetry

MDPI

Article

ECCPoW: Error-Correction Code based Proof-of-Work for ASIC Resistance

Hyunjun Jung [1] and Heung-No Lee [2,*]

1 Blockchain Internet Economy Research Center, Gwangju Institute of Science and Technology, Gwangju 61005, Korea; junghj850@gist.ac.kr
2 School of Electrical Engineering and Computer Science, Gwangju Institute of Science and Technology, Gwangju 61005, Korea
* Correspondence: heungno@gist.ac.kr; Tel.: +82-62-715-2237

Received: 20 May 2020; Accepted: 5 June 2020; Published: 9 June 2020

check for updates

Abstract: Bitcoin is the first cryptocurrency to participate in a network and receive compensation for online remittance and mining without any intervention from a third party, such as financial institutions. Bitcoin mining is done through proof of work (PoW). Given its characteristics, the higher hash rate results in a higher probability of mining, leading to the emergence of a mining pool, called a mining organization. Unlike central processing units or graphics processing units, high-cost application-specific integrated circuit miners have emerged with performance efficiency. The problem is that the obtained hash rate exposes Bitcoin's mining monopoly and causes the risk of a double-payment attack. To solve this problem, we propose the error-correction code PoW (ECCPoW), combining the low-density parity-check decoder and hash function. The ECCPoW contributes to the phenomenon of symmetry in the proof of work (PoW) blockchain. This paper proposes the implementation of ECCPoW, replacing the PoW in Bitcoin. Finally, we compare the mining centralization, security, and scalability of ECCPoW and Bitcoin.

Keywords: error-correction codes proof-of-work (ECCPoW); proof-of-work (PoW); ECCPoW implementation; ASIC resistance

Green Bitcoin: Global Sound Money

Heung-No Lee, Young-Sik Kim, Dilbag Singh, and Manjit Kaur

Abstract

Modern societies have adopted government-issued fiat currencies many of which exist today mainly in the form of digits in credit and bank accounts. Fiat currencies are controlled by central banks for economic stimulation and stabilization. Boom-and-bust cycles are created. The volatility of the cycle has become increasingly extreme. Social inequality due to the concentration of wealth is prevalent worldwide. As such, restoring sound money, which provides stored value over time, has become a pressing issue. Currently, cryptocurrencies such as Bitcoin are in their infancy and may someday qualify as sound money. Bitcoin today is considered as a digital asset for storing value. But Bitcoin has problems. The first issue of the current Bitcoin network is its high energy consumption consensus mechanism. The second is the cryptographic primitives which are unsafe against post-quantum (PQ) attacks. We aim to propose Green Bitcoin which addresses both issues. To save energy in consensus mechanism, we introduce a post-quantum secure (self-election) verifiable coin-toss function and novel PQ secure proof-of-computation primitives. It is expected to reduce the rate of energy consumption more than 90 percent of the current Bitcoin network. The elliptic curve cryptography will be replaced with PQ-safe versions. The Green Bitcoin protocol will help Bitcoin evolve into a post-quantum secure network. In addition, it improves the properties of Bitcoin's hash PoW while addressing environmental concerns.

Keywords: Bitcoin, energy consumption, error-correction codes, post-quantum security, sound money, verifiable random function

I. INTRODUCTION

WE the global citizens not by our choice live in a world of boom-and-bust cycles created by the Federal Reserve Board (FED) of the United States. In the boom phase of a cycle, the FED supplies debt-mon-

Papers are available at Docsend.

Unique Tech Stack

We have been building My AI Agents!

Legal AI = Legal QA Corpus + LLaMa3 + Fine Tuning + RAG

IEEE Access

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2023.DOI

Catalyzing Legal Discourse: A Comprehensive Evaluation of LQA-RAG in the Legal Domain

RAHMAN S M WAHIDUR [1], SUMIN KIM [2], DAVID SAMUEL BHATTI[1] and HEUNG-NO LEE [1], (Senior Member, IEEE)

[1]School of Electrical Engineering and Computer Science, Gwangju Institute of Science and Technology, Gwangju 61005, South Korea
[2]Artificial Intelligence Graduate School, Gwangju Institute of Science and Technology, Gwangju 61005, South Korea

Corresponding author: Heung-No Lee (heungno@gist.ac.kr).

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No.2023-2021-0-00118, Development of decentralized consensus composition technology for large-scale nodes) and This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC (Information TechnologyResearch Center) support program (IITP-2023-2021-0-01835) supervised by the IITP (Institute of Information & CommunicationsTechnology Planning & Evaluation)

ABSTRACT

Legal practice has seen a significant increase in the adoption of products leveraging artificial intelligence (AI) for various core legal tasks. However, these technologies are still in their early stages and currently lack the capability to effectively address domain-specific challenges. One promising approach is retrieval-augmented generation (RAG), which enhances response quality by integrating a curated external knowledge base into the large language model (LLM) prompt. This paper presents a detailed evaluation of RAG for legal natural language processing (NLP) to assess its effectiveness in this domain. The empirical study encompasses a diverse range of challenging datasets, spanning from 50 to 97,000 samples, and addresses six major NLP tasks: text classification, multiple-choice, sentence completion, semantic understanding, information retrieval, and question answering. Initially, the general-purpose embedding model was trained using legal corpora and observed a performance improvement ranging from 13.5% to 15.5% compared to its baseline models. Furthermore, comparisons were made between general domain LLMs and a hybrid fine-tuned model (HFM) specifically designed for the legal domain, demonstrating performance improvements ranging from 3.33% to 45% across various tasks. Finally, the evaluation of the proposed LQA-RAG architecture against other configurations shows that the RAG model significantly outperforms all baseline models across multiple metrics. The experiments suggest that using domain-specific fine-tuned LLMs and advanced RAG modules with a feedback function enhances the performance of legal RAG, surpassing general domain models across diverse tasks. This finding can aid legal NLP practitioners by suggesting suitable methods for diverse tasks and illuminating future research directions in the field.

INDEX TERMS LAW, Retrieval Augmented Generation, Fine-tuning.

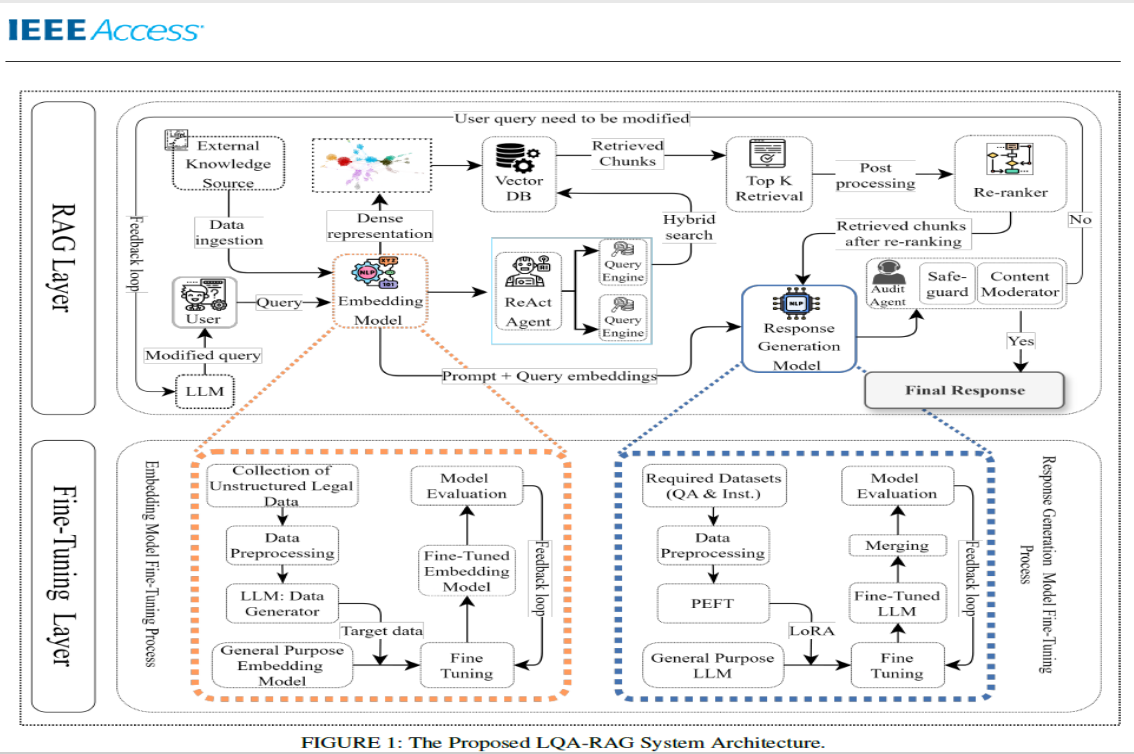


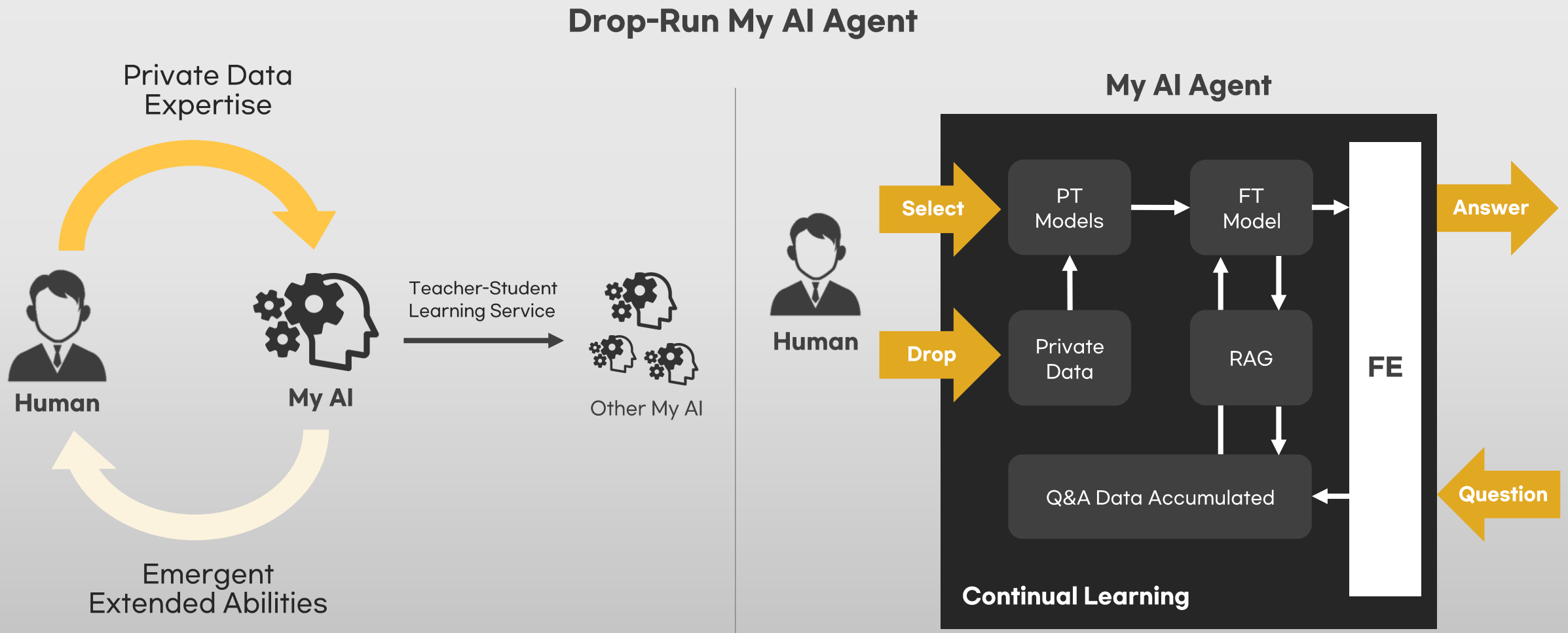
FIGURE 1: The Proposed LQA-RAG System Architecture.

Comparison to open source base models such as LLaMa3 and FlanT5,

our legal AI assistant shows superior performance in all measures!

Unique Tech Stack

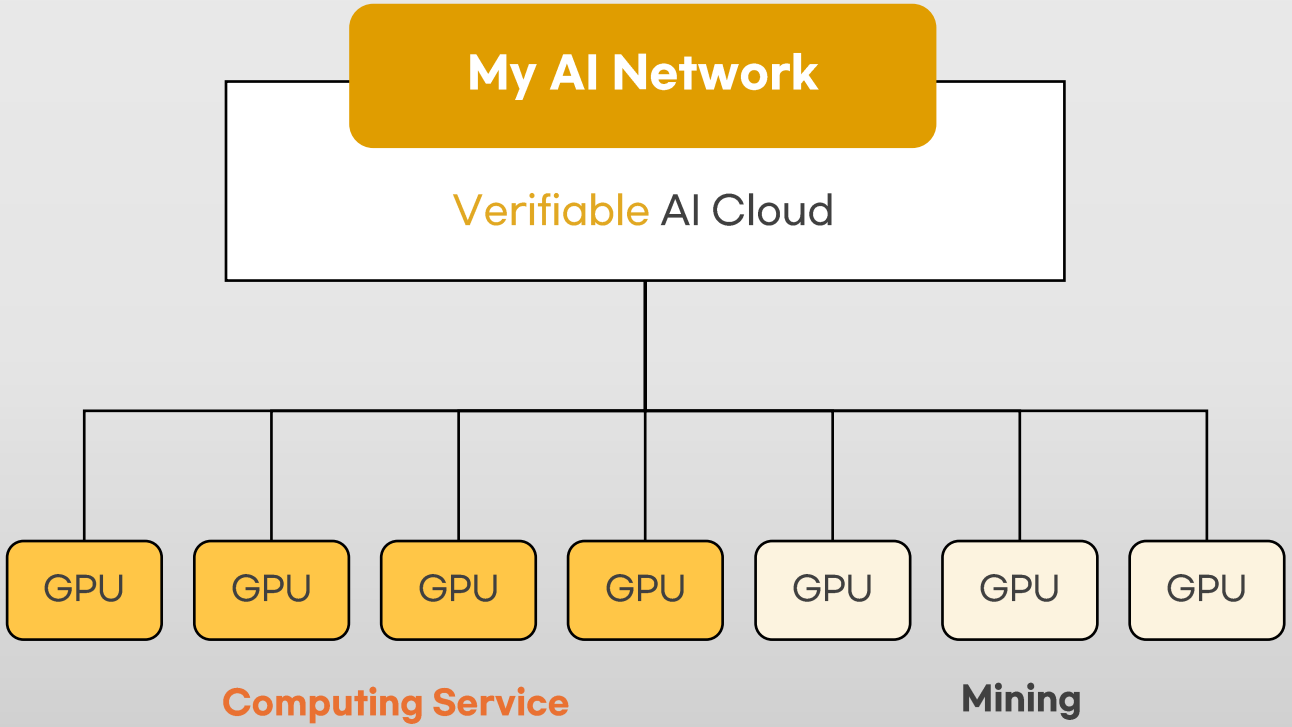
Drop-Run AI Agent : Grow your own AI and let it interact with others.



LiberVance

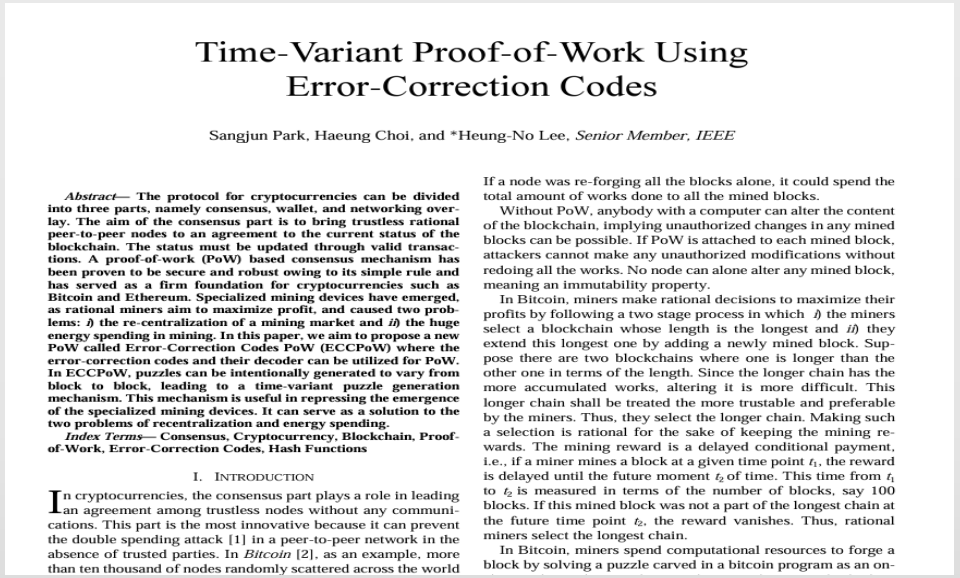
Unique Technical Stack

Our solution package can upgrade a blockchain in to a verifiable AI Compute Cloud!



Novel Consensus Layer

- Error Correction Code VCA ▶ ASIC resistance & promote GPU nodes
- Verifiable Coin Toss ~ Random self election ▶ **Mining** vs **Computing Service**



Time-Variant Proof-of-Work Using Error-Correction Codes

Sangjun Park, Haeung Choi, and *Heung-No Lee, *Senior Member, IEEE*

***Abstract*— The protocol for cryptocurrencies can be divided into three parts, namely consensus, wallet, and networking overlay. The aim of the consensus part is to bring trustless rational peer-to-peer nodes to an agreement to the current status of the blockchain. The status must be updated through valid transactions. A proof-of-work (PoW) based consensus mechanism has been proven to be secure and robust owing to its simple rule and has served as a firm foundation for cryptocurrencies such as Bitcoin and Etherum. Specialized mining devices have emerged, as rational miners aim to maximize profit, and caused two problems: *i*) the re-centralization of a mining market and *ii*) the huge energy spending in mining. In this paper, we aim to propose a new PoW called Error-Correction Codes PoW (ECCPoW) where the error-correction codes and their decoder can be utilized for PoW. In ECCPoW, puzzles can be intentionally generated to vary from block to block, leading to a time-variant puzzle generation mechanism. This mechanism is useful in repressing the emergence of the specialized mining devices. It can serve as a solution to the two problems of recentralization and energy spending.**

***Index Terms*— Consensus, Cryptocurrency, Blockchain, Proof-of-Work, Error-Correction Codes, Hash Functions**

I. Introduction

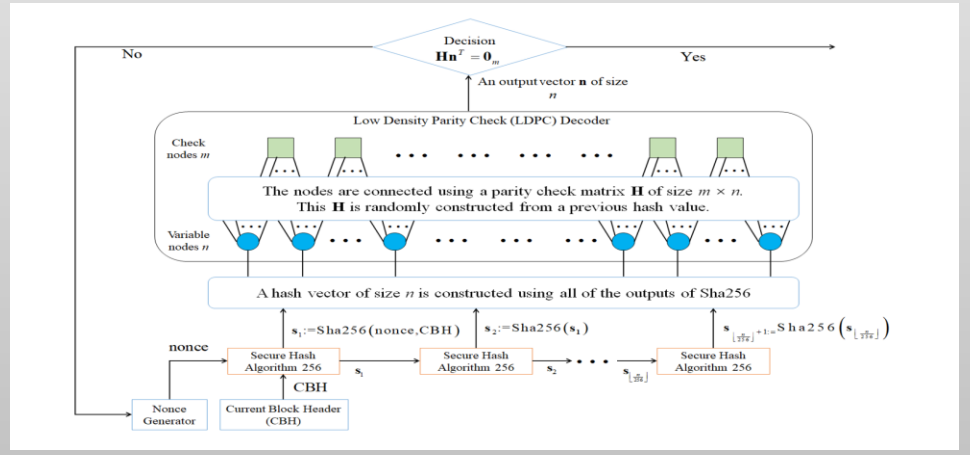
In cryptocurrencies, the consensus part plays a role in leading an agreement among trustless nodes without any communications. This part is the most innovative because it can prevent the double spending attack [1] in a peer-to-peer network in the absence of trusted parties. In *Bitcoin* [2], as an example, more than ten thousand of nodes randomly scattered across the world

If a node was re-forging all the blocks alone, it could spend the total amount of works done to all the mined blocks.

Without PoW, anybody with a computer can alter the content of the blockchain, implying unauthorized changes in any mined blocks can be possible. If PoW is attached to each mined block, attackers cannot make any unauthorized modifications without redoing all the works. No node can alone alter any mined block, meaning an immutability property.

In Bitcoin, miners make rational decisions to maximize their profits by following a two stage process in which *i*) the miners select a blockchain whose length is the longest and *ii*) they extend this longest one by adding a newly mined block. Suppose there are two blockchains where one is longer than the other one in terms of the length. Since the longer chain has the more accumulated works, altering it is more difficult. This longer chain shall be treated the more trustable and preferable by the miners. Thus, they select the longer chain. Making such a selection is rational for the sake of keeping the mining rewards. The mining reward is a delayed conditional payment, i.e., if a miner mines a block at a given time point t_1, the reward is delayed until the future moment t_2 of time. This time from t_1 to t_2 is measured in terms of the number of blocks, say 100 blocks. If this mined block was not a part of the longest chain at the future time point t_2, the reward vanishes. Thus, rational miners select the longest chain.

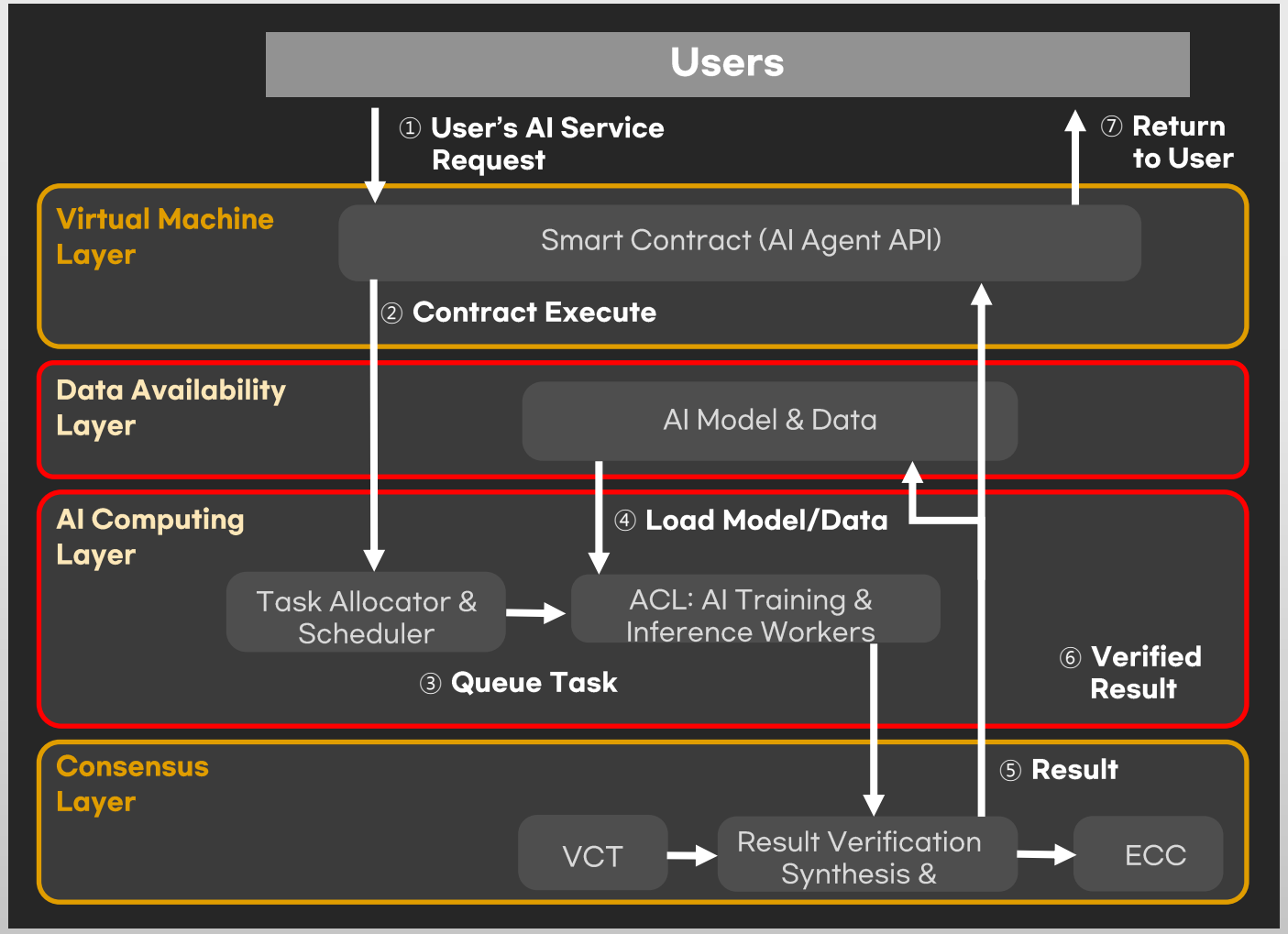
In Bitcoin, miners spend computational resources to forge a block by solving a puzzle carved in a bitcoin program as an on-



Paper PDF

Unique Tech Stack

Novel AI Compute Module interacts with smart contract and consensus layer.



AI Compute Module Procedure

1. User makes AI service request to Smart Contract.
2. Blockchain executes the smart contract
3. AI-layer allocates AI task to the AI computing layer (ACL)
4. ACL loads model & data. It does the AI compute task each and every block until the task is completed.
5. When the task is completed ACL returns the compute result to the C-layer.
6. C-layer verifies the compute result.
7. If result verification comes out positive, C-layer proceeds to the consensus (e.g., POS or POW) stage.
8. If the requested task is completed, C-layer notifies SC, which makes payment and returns the result to the user.

Unique Tech Stack

We can build a network of decentralized verifiable data storage and GPU nodes.

Global L1 Blockchain

My AI Network

Verifiable AI Compute Cloud

Distributed Ledger
for Tx & contract

Data Cloud
for AI model & data

GPU GPU GPU GPU GPU GPU

AI Computing Cloud
for AI Training & AI Inferences

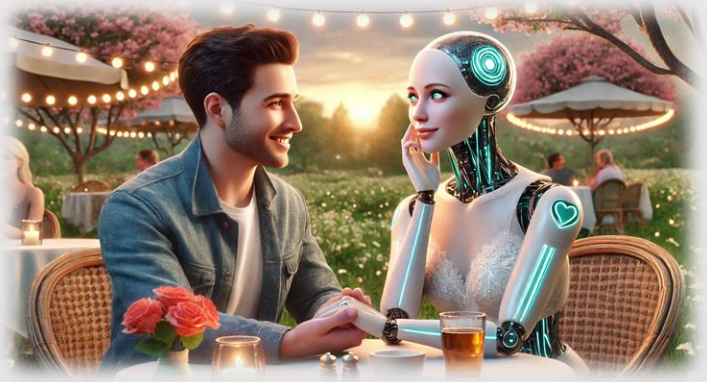
GPU GPU GPU GPU

Consensus
for Security & Verifiability

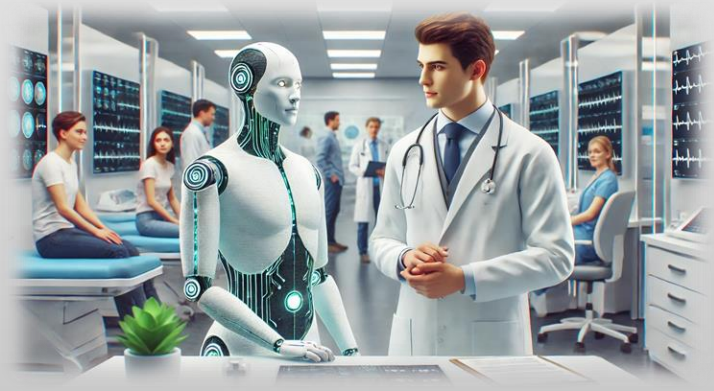
My AI Network is a public L2 chain with nodes scattered around the globe.

Use Cases

Personal Assistant



Social Companion



Medical Assistance

Legal Assistance

Use Case: Radiologist AI

My AI Agent provides service to other agents and earns income!

Monetize your expertise, overcoming barriers of time and state borders!

- Harvard medical center is known for AI agents trained with a large corpus of colonoscopy polyp images.
- Korean clinical doctor sees an American visitor and sends out an exam request to the radiologist AI agent.

Clinical Doctor, Seoul
Seeing American patient

Seoul, RoK

Clinical Doctor
AI Agent

① Exam Request

② Diag Results

③ Money

Cambridge, MA

Harvard Medical Center
Radiologist AI Agent

My AI Network

My AI Network Demo Video

Team / Why us

Prof. Heung-No Lee **CEO / Founder**

- Tenured Professor at GIST
- Editorial Board Member of IEEE Trans. Cybernetics
- Director of Blockchain Intelligence Convergence Center
- Former Professor at the Univ. of Pittsburgh
- PHD/MS/BS, UCLA, USA

Prof. Young-Sik Kim

CTO

- Cryptography Expert
- PHD/MS/BS, Seoul National Univ.

Sung-Jin Cho

CMO

- Marketing Expert
- B.S., GIST

10+ Researchers

PHD/MS/BS, GIST

- Blockchain / Crypto
- AI / Web3

Affiliation

Ministry of Science and ICT
GIST
Google Cloud
DLG
SEOUL NATIONAL UNIVERSITY
UCLA
KDI SCHOOL
KDI School of Public Policy and Management
kt
The University of Texas at Austin School of Law
UNIVERSITY AT ALBANY
STATE UNIVERSITY OF NEW YORK
HUFS
HANKUK UNIVERSITY OF FOREIGN STUDIES
DGIST 대구경북과학기술원
Daegu Gyeongbuk Institute of Science & Technology

Will continue to be added !

Release Plan

We plan three phases for full Release.

Q4 2024

Testnet + Drop-Run
My AI agent

Q1 2025

AI Compute Module

Q2 2025

My AI Network
Protocol

Q3 2025
Full Release

To the Moon

Three phases with three upgrades
can create expectations for steady network value growth!

100,000 nodes
10,000 AI agents

My AI Network

Let us build a global AI agent network that **empower people!**

LiberVance