Exclusion Clause

Foreword

Introduction

The problems

Limitation

Mining

Practical Difficult in AI Researches

Ou r vision

Our Mission

BIGO Architecture : AI Ecosystem on Block-chain

The Key Technologies of BIGO

Summary

AI Deep learning

AI Mining

BIGO AI BIGO Bushiness Model

The Art of AI BIGO

Proof of Learning (POL)

Distributed GPU Network

ERC20?

ERC721?

BIGO Ecosystem Use Cases

BIGO Coins

Distribution Mechanism

Proceeds Allocation

Plans for Burning?

Future plans

Roadmap

Exchange Listing

Future

Team member and Advisory

Contact

# Introduction

Artificial intelligence (AI) refers to the ability of computers to think and decide like humans. In most time of human history, AI only exists as a concept until the computer was created. The advent of machine learning (ML) indicated AI tech a great forward step. With tremendous ability of centralized entity such as e-commerce and social media organization to collect enormous amount of data from their customers, ML can learn from their experience continuously, thus refining their methods and methodologies to accurately target their customers. However, the centralized nature of AI may lead to the possibility of data tampering, as data can be subject to hacking and manipulation as it is managed and stored in centralized manner. Moreover, the data provenance and authenticity of the sources generating the data are not guaranteed. This may lead to AI decision outcomes highly erroneous, risky, and dangerous. In other words, we face a series of challenges such as security, privacy and reliability as AI used in a traditional, centralized system.

Blockchain as an emerging technology to realizing the distributed ledgers has attracted extensive research attention recently. Such a ledger intends to achieve decentralized transaction management, which means that any node joining the ledger can initiate transactions equally according to rules, and the transaction does not need to be managed by any third party. All transactions in the system are stored in blocks, which are then linked as a chain and organized in chronological order. Moreover, transactions that have written in blocks are immutable and transparent to all peers. With all these attractive characteristics, blockchain is drastically different from the traditional centralized trust entities. In recent years, the blockchain has developed rapidly. In 2009, a decentralized currency called Bitcoin was for the first time implemented in practice by Satoshi Nakamoto. In 2013, the next-generation smart contract and decentralized application platform called Ethereum was created by Vitalik Buterin, followed by the emerging permissioned blockchain. Due to the characteristics such as decentralization, persistency, anonymity and auditability of emerging Blockchain, it is able to solve many problems in centralized or distributed systems. And because we can get traceable big data on Blockchain, It has been leveraged with AI to apply in different fields like cryptocurrency, healthcare, supply chains, financial services, etc. Some of the significant features of leveraging Blockchain for AI can be summarized as follows:

* Enhanced Data Security. Information held within blockchain is highly secure. Blockchains are very well known for storing sensitive and personal data in distributed environment without single point of failure. Blockchain databases hold data that are digitally signed. This allows AI algorithms to work on secure data, and thereby ensuring more trusted and credible decision outcomes.
* Improved Trust on Robotic Decisions. Recording the decision making process of an AI system on a blockchain would increase transparency and it would gain public trust to understand the robotic decisions. The need for a third party auditor can be eliminated in a swarm robotic ecosystem, where the consensus in the swarm can be achieved through an absolutely decentralized approach.
* Collective Decision Making. In a robotic swarm ecosystem, all the agents need to work in coordination to achieve the swarm goal. The decentralized decision-making algorithms have been adopted in many robotic applications, without the need for a central authority. Robots take decisions by voting and outcomes are determined by majority rules. Each robot can cast its vote in the form of a transaction, where blockchain is public for all robots which can be utilized for verification of voting results. This process is repeated by all robots until the swarm comes to a decisive conclusion.
* Decentralized Intelligence. For taking smart high level decisions which involve multiple agents to perform different subtasks that have access to the common training data, different individual cybersecurity AI agents can be combined to provide fully coordinated security across the underlying networks and to solve scheduling issues.
* High Efficiency. Multi-user business processes, involving multiple stakeholders such as individual users, business firms, and non-profit organizations, are inherently inefficient due to multiparty authorization of business transactions. The integration of AI and blockchain technologies enables intelligent Decentralized Autonomous Agents (or DAOs) for automatic and fast validation of data/value/asset transfers among different stakeholders.

The consolidation of AI and blockchain can create secure, smart and decentralized system for the highly sensitive information. In the next chapter, we will discuss some problems and challenges we face when we apply blockchain for AI.

## The problems

Although Blockchain has such benefits that it is usually regarded as better choices than centralized or distributed system in many cases when leveraged for AI, it is certain that the combination of Blockchain and AI still has some challenges raging from society to technology. Undoubtedly, there is no simple strategy to solve all problems. Here we only focus on technical challenges and pose the limitation of some current technologies on Blockchain.

### Scalability

With the domination of Bitcoin in cryptocurrency, the scalability issues of blockchain were exposed. According to previous research, the maximum throughput and latency are the two most important performance metrics that have a significant impact on the user’s quality of experience (QoE).

Among all metrics, transaction throughput receives the most attention. It has been reported that Bitcoin’s highest transaction throughput is 7 TPS (transaction per-second) while Visa can achieve more than 4000 TPS. Ethereum’s transaction throughput is up to 15 TPS, a bit more than Bitcoin’s, but still far behind centralized system's. As blockchain leveraged for AI, the need for throughput may soar because low throughput probably cause long delay or even failure in decentralized applications (DApps). Obviously, low throughput of blockchain cannot satisfy the large-scale application scenarios.

In theory, throughput is restrained by the block interval and the block size. A larger block can store more data, directly raising throughput, but it also causes an increase in block propagation time and the need for a larger storage space. To ensure the current block to be propagated to most peers in the whole network before the next block is generated, which is critical to reducing the probability of fork, the block size and the average block interval between two successive blocks should be well configured. In Bitcoin, the block interval is about 10 minutes, and the block size is around 1 MB, which limits the number of transactions that can be stored in each block, while the number is 15-20 seconds and 20-30 KB respectively in Ethereum. Thus, to maintain the block propagation time while increasing the block size, the average bandwidth of the whole system that determines the block propagation time becomes a performance bottleneck of the blockchain system.

### Latency

Another metric, transaction confirmation latency that is the time for a transaction to be confirmed, also has a strong relation with user experience. Due to the huge volume of Bitcoin or other cryptocurrency transactions nowadays, the limited size of blocks is far from enough to deliver all transactions submitted by nodes. Under such a situation, miners tend to select transactions that are with high transaction fees. As a result, the transactions that are with a low bid have to wait until packaged, which leads to the longer transaction latency.

Ethereum, another popular PoW-featured blockchain makes this problem even severe since some popular DApps embeding AI in Ethereum have induced extensive congestion in the entire network. As we can see in Figure 1, the total number of Ethereum transactions waiting to be confirmed in a certain period maintains a high level.

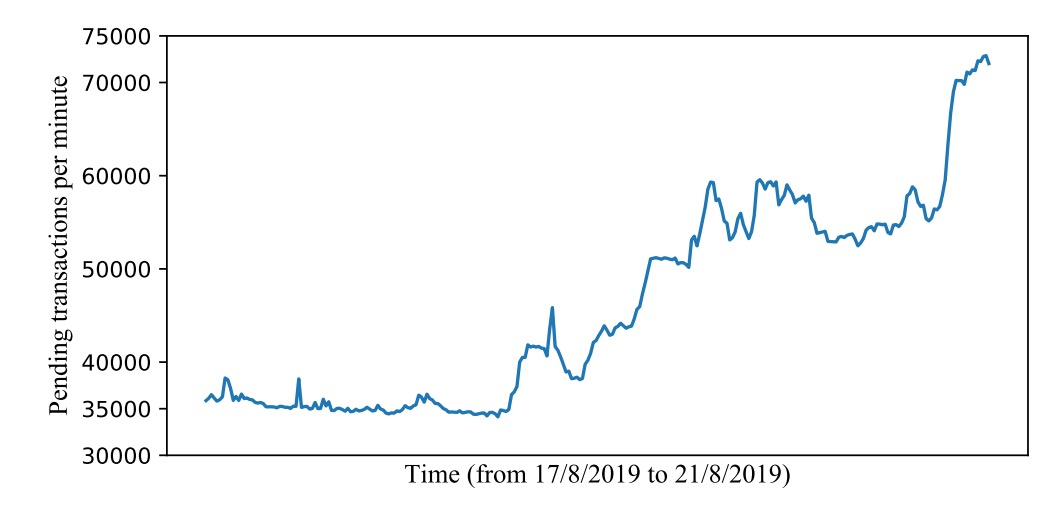


Figure 1 Pending transactions per minute in Ethereum

### Storage

Besides the performance bottleneck of blockchain, we should also consider the capacity problem of blockchain seriously. As the scale of a blockchain growing rapidly, the storage required by all blocks grows accordingly. Therefore, the full nodes, which store all block data of the network, are required large storage capacity for each. You might consider increasing total size of blockchain is always a good thing for AI since AI is able to access to much more reliable data. However, the Bootstrap time will increases linearly as the blockchain history grows, slowing down the process of new nodes joining into the system. As we see in Table 1, which indicates the total size of two blochcains at the time of writting, Ethereum, a blockchain containing DApps leveraged for AI, take up 10 more times than traditional cryptocurrency system Bitcoin, thus it makes the problem more severe. All these restrictions degrade the availability and decentralization of a blockchain, and thus should be examined closely when developing a large-scale blockchain.

Table 1 Total size of the blockchains

|  |  |
| --- | --- |
| Blockchain | Total size of the blockchain (approx. in GB) |
| Bitcoin | 323 |
| Ethereum | 4233 |

Nowadays, more block compression methods have been proposed to reduce redundant data of blocks, which is beneficial for easing the capacity problem. At the same time, sharding techniques, partitioning the whole blockchain network into different shards, have been researched more detailed to solve the capacity problem of blockchain.

### Energy consumption

Meanwhile, many concerns have been raised about the energy consumption of Proof-of-work based blockchain systems, such as Bitcoin and Ethereum. Miners in a PoW-featured blockchain are always competing with each other through calculating, which results in a large dissipation of electricity. Figure 2 Energy Consumption by Country inc. Bitcoin & Ethereum shows the energy consumption of Bitcoin and Ethereum comparing with some countries/organizations, where we can find that the entire blockchain network consumes even more energy than many countries, such as Pakistan and Belgium, and barely ranks the 34th. Although PoW works securely, it’s far from green enough to be a sustainable consensus mechanism for future blockchain.

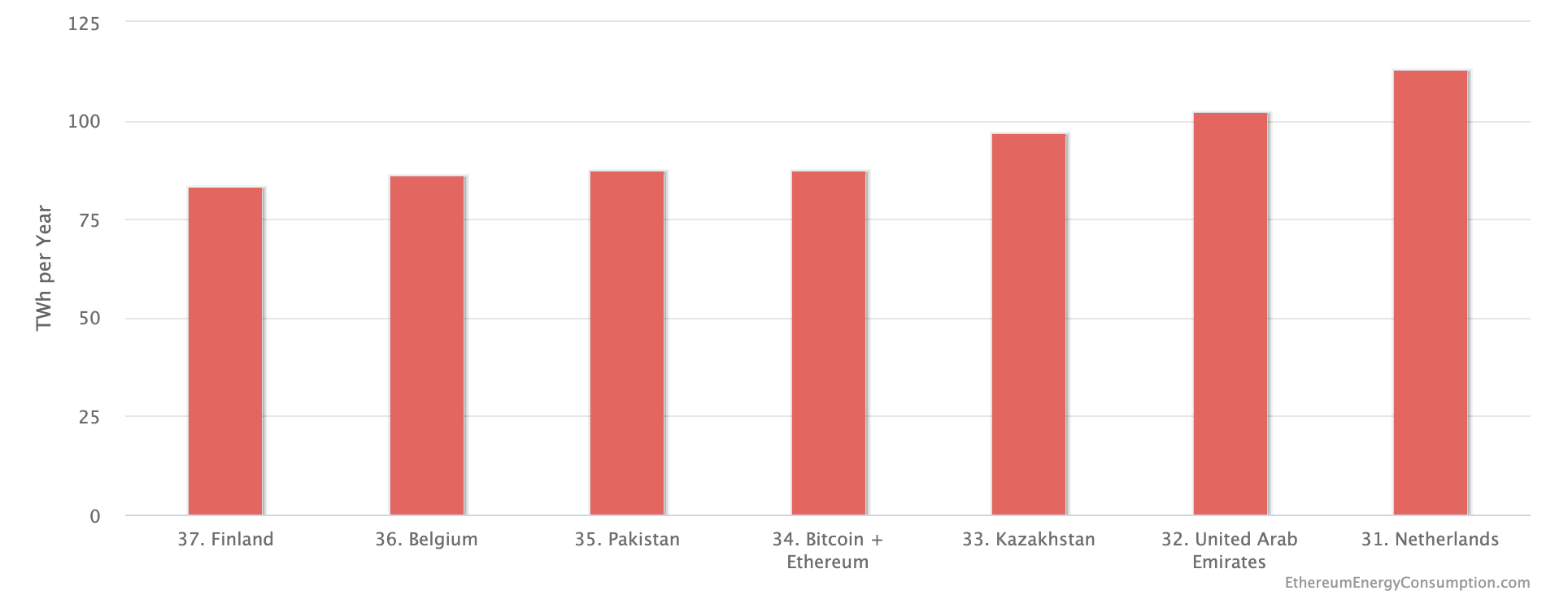


Figure 2 Energy Consumption by Country inc. Bitcoin & Ethereum

### Blockchain Security

The decentralized power found in blockchain can suffer from abuses and misuses. Though blockchain provides robust schemes for securing IoT and predictive analysis, the blockchain systems are vulnerable to cyber-attacks as that of 51% attack. The consensus mechanism depending upon the hashing power of the miner can be compromised, in which the decentralized platform becomes centralized around a few mining farms that control consensus and settlement finality. This security problem is more evident in public Blockchain such as Ethereum and Bitcoin. Private blockchain platforms suffer less from this problem, as consensus protocols are predefined among parties. Furthermore, the execution environment of the mining nodes is not protected, especially for private blockchain platforms with a few mining nodes as that of Hyper- ledger, in which the execution outcomes can be tampered with. To remedy this problem, newly emerging blockchain platforms are equipped with hardware to offer execution in a Trusted Execution Environments (TEEs).

### Smart Contracts Vulnerabilities and Deterministic Execution

It is crucial to ensure that the implementation of a smart contract is free of bugs and vulnerabilities and secure against attacks. It is important to safeguard the code and the information on the network, as they may be vulnerable to attacks. For example, the smart contract for the DAO which was built on the Ethereum platform had serious code vulnerability and was hacked in 2016. This resulted in a loss of 3.6 million Ethers. There is a definite need for blockchain engineering, addressing this issue posed by smart contract programming and other applications running on blockchain. The vulnerability issues are due to poor and negligent programming practices in the languages used to write the smart contracts code (as that of Solidity and Chaincode). Testing smart contracts for vulnerabilities has become of a critical importance, and some tools have been developed to assess the security state of a smart contract code. Furthermore, as of today, the execution outcomes of smart contracts are all deterministic and cannot be probabilistic. This can pose a key challenge for decentralized AI in which AI and machine learning-based decision making algorithms get executed as smart contracts by the mining nodes, in which the execution outcome are not usually deterministic, but rather random, unpredictable and most often approximate. This entails a novel solution to deal with approximate computation and to devise consensus protocols for mining nodes for agreeing on results with a particular degree of certainty, accuracy, or precision, and with data input that might be highly fluctuating as that of IoT and sensory readings.

## Limitation

Undoubtedly there is no simple strategy to solve all problems stated above. Actually, after numerous studies on the particularities of blockchain, some researchers raise the view of Blockchain Trilemma. Similar to the CAP theory in the traditional field of the distributed system, the Blockchain Trilemma points out that three important properties of a blockchain system, involving decentralization, security, and scalability, cannot perfectly co-exist. In other words, if we guarantee Blockchain’s characteristics of decentralized and security, we are unable to ensure the scalability, an important indicate of users’ quality of experience.

However, as we combine blockchain with AI, the importance of scalability is much more prominent. Without high throughput and low delay, AI cannot respond on time, which may cause robotic failure in decentralized blockchain system. In order to improve the scalability of the blockchain, the properties of blockchain i.e. decentralization and security must be sacrificed to some extent. To keep balance among them, many companies and research teams have proposed a large number of different solutions. We classify them according to the hierarchical structure of blockchain. In detail, the hierarchical structure mainly includes two layers, which are described briefly as follows. Layer1 focuses on the on-chain design of blockchain including the structure of blocks, consensus algorithm and also the specific structure of the main-chain, while Layer2 concentrates on off-chain methods, which intends to reduce the burden of the main-chain, such as executing some transactions off-chain and moving some complex computational tasks to an off-chain platform. Layer1 (on-chain) solutions such as Bitcoin-Cash increasing the block size, Compact block relay compressing the blocks, Sharding techniques, and various improved consensus algorithms, in which the transaction throughput is increased and transaction latency is decreased, respectively. Layer2 solutions like payment channel Bitcoin’s Lightning network and side chain (Plasma of Ethereum) are still under developing. The cross-chain solutions that emerged in the last few years also play an important role in Layer2 scaling solutions. In summary, with both advantages and limitations, those solutions are striving to achieve decentralization, security, and scalability simultaneously.

In this paper, we mainly concentrate on the limitation of some of the current exist consensus algorithms classified as Layer1 (on-chain) solutions and discuss how they can impact the performance of AI applications on blockchain.

### PoW

Proof of Work (PoW) is an original consensus algorithms introduced by the anonymous founder of Bitcoin- Satoshi Nakamoto. The mechanism behind proof of work was a breakthrough in the space because it simultaneously solved two problems. First, it provided a simple and moderately effective consensus algorithm, allowing nodes in the network to collectively agree on a set of canonical updates to the state of the Bitcoin ledger. Second, it provided a mechanism for allowing free entry into the consensus process, solving the political problem of deciding who gets to influence the consensus, while simultaneously preventing sybil attacks.

Although PoW proved to be highly adopted consensus protocol, in large networks it consumes gigantic amount of energy and increases delay in transaction approvals. AI applications have high frequency of write operations because the intelligent algorithms continuously update the decision structures for informed decisions. Therefore, PoW protocols become performance bottleneck in real-time AI applications.

### PoS

Proof of stake (PoS) is a consensus algorithm designed and developed to address some of the trade-offs of the PoW algorithm. The block-producing node is determined by an application of mathematical function involving a few determining factors, such as the stake (for example, ETH), the age of the node, and the randomization of eligible node candidates.

PoS proved to be energy-effcient when compared with PoW and it also indirectly solves the security problem by stopping the anonymous validators and allowing only those validators who own the native currency of the blockchains. However, the validators have nothing to lose on the blockchain if they do not validate the transactions; therefore, it may cause delay while creating new blocks. PoS could be useful for delay tolerant AI applications but these protocols are not suitable when AI applications need to handle streaming data, detect changes, and performed real-time informed decisions.

### PoB

Proof of Burn (PoB) is a consensus algorithm with an interesting approach to solving transition problems from one version of cryptocurrency to another in the blockchains. Through the PoB algorithm, the old cryptocurrency (or its preceding version) is burnt in order to reduce its supply and gradually increase the supply of the new cryptocurrency (or its succeeding version). This consensus algorithm is practiced in various forms, including a method wherein users can transfer the old cryptocurrency to an unspendable wallet address in exchange for new ones.

PoB benefits the users by allowing them to invest initially and create their stake on the blockchain and become authorized validators. It also solves the energy consumption problem of PoW. In addition, coin burning strategy reduces the number of coins on the blockchain. Therefore, coin value increases gradually. Coin burning also benefits in balancing the number of coins on the blockchain, spending unsold coins, and paying for transaction fees on the network. AI applications can harness PoB protocols if they want to incentivize the users in order to maintain the value of underlying decisions. For example, the applications which need to maintain a specific level of accuracy, a certain number of clusters, or minimum number of objects to be found, can burn the learning models and search trees in order to maintain the value across the blockchain. However, the PoB algorithm is usually applicable in PoW-based blockchains and so has a limitation of applicability. This is due to the requirement of verifiable proofs and the ability to decay the burnt coins over time, which is naturally capable through PoW algorithms.

### PoAc

The Proof of Activity (PoAc) protocol is a hybrid of PoW and PoS. This protocol initially works on empty blockchains using PoW algorithm and solves the 51% attack problem. Initially, PoAc protocol solves complex mathematical problems and the validators start receiving the rewards which increases their stake on blockchains. The protocol then enables PoS algorithm for validators having acceptable stake on the blockchain. PoAc has been proven to be efficient in terms of security, storage, and network communication. Therefore, it could become handy for AI applications requiring less data availability and more security.

## Mining

In the decentralized currency system like Bitcoin and Ethereum, we need to combine the state transition system with a consensus system in order to ensure that everyone agrees on the order of transactions. This process called mining is used to secure and verify the transactions on the blockchain. The necessity of mining to security will not be repeated in this paper and the mechanism of mining will be discussed here. In the mechanism of mining on Bitcoin and Ethereum, PoW is used to determine the validity of miner’s work. As we discussed before, PoW is energy-intensive and not suitable for AI DApps although it is a relatively safe way. Besides, as we stated above, other existing consensus algorithms have their limitations on blockchain combined with AI. Here a smarter mining process named AI mining will be proposed and it will be discussed in detail at later chapters .

### AI Mining

At the beginning of the Introduction, we discuss a series of applications about the combination of blockchain and AI. In general, AI can benefit from the availability of many blockchain platforms for executing machine learning algorithms and tracing data that are stored on decentralized P2P storage systems. This is only one way combining blockchain and AI. On the other hand, blockchain can also benefit from AI by implementing machine learning algorithms to improve throughput and decrease delay of blockchain. In this paper, a new consensus proof based on quality of learning will be introduced in later chapter. In the blockchain, a new AI layer is attached on a block, which enable all other nodes get to know who complete the learning process first.

In summary, AI mining can be more energy efficient, less delay and much faster than traditional honest mining, and it also decreases the centralized mining pool. It is a promising solution for current blockchain problems and thus the blockchain using AI mining is suitable for future DApps.

### Switch algorithms

As we discussed above, there are a number of consensus algorithms and each has its advantages and limitations. Undoubtedly, a large plethora of research opportunities are available for future researchers to explore if the application level consensus protocols could be designed considering proofs based on quality of learning models, efficient search strategies, quality and provenance of data, and quality of optimization. A smart mining process should be adapted to various consensus protocols raging from PoW to future proofs including Proof of Learning. Therefore, a switch algorithm is proposed here to work in different environment. The process can be described in the following step:

1. Implement AI deep learning algorithm to learn the data from the blockchain;

2. Train AI to distinguish which mining strategy cost least;

3. Choose the probable optimal mining strategy i.e. AI mining, honest mining…

With this mining process, the algorithm can be used in existing blockchain like Ethereum thus the compatibility of AI mining can be guaranteed.