The next generation high-efficiency, secure, developer friendly Cyber-Smart OS
Background

Existing public blockchains and smart contract platforms are known to have scalability and security issues. TPS is low to $\leq 10$. Vulnerable smart contracts become so common that big hacking events happen every month. In addition, no current solutions satisfy the demand for processing high volume of data in parallel and securely.

We present EON — a new blockchain platform that is designed to scale and to be safe. As the number of nodes grow in number, the processing capacity of the whole blockchain network actually increase. The cornerstone in EON’s design is the idea of sharding, Verifiable Random Function (VRF) and Practical Byzantine Fault Tolerance (PBFT) which enables the whole network to split the work into pieces to fully utilize computing potential of each node.

EON further proposes formal verification based smart contract language, modularized libraries as well as HTML++ so that the developers can write fast, parallel and secure code to support real world computing problems such as AI computing or large-scale real-time human collaboration tasks.
CONTENTS

BACKGROUND ......................................................................................................................... 1

1. INTRODUCTION .................................................................................................................. 3
   1.1 RESTRUCTURING THE INTERNET .................................................................................. 3
   1.2 FINAL GENERATION BLOCKCHAIN ............................................................................. 3

2. EON OVERVIEW .................................................................................................................. 5

3. VIRTUAL CLOUD COMPUTING ....................................................................................... 7
   3.1 INFINITE DECENTRALIZATION CONCEPT ................................................................. 7
   3.2 THRESHOLD RELAY ..................................................................................................... 8
   3.3 MULTI-LAYER CLOUD ............................................................................................... 8

4. SUPER VIRTUAL COMPUTER ............................................................................................ 9
   4.1 AI IS LAW .................................................................................................................... 9
   4.2 SVC DRIVE MECHANISM ........................................................................................... 9
   4.3 MULTILAYER NEURAL NETWORKS ............................................................................ 10

5. CONSENSUS LAYER ......................................................................................................... 11
   Overview ........................................................................................................................... 11

6. SMART CONTRACT PROTOCOL LAYER .......................................................................... 17

7. SECURITY & APPLICATION LAYER .................................................................................. 19

9. TOKEN ECONOMICS SYSTEM AND INCENTIVIZATION ................................................. 22

10. COMMUNITY & PLATFORM FEATURES ......................................................................... 22

11. ROADMAP ....................................................................................................................... 23

12. TOKEN ALLOCATION ...................................................................................................... 23

13. TEAM ............................................................................................................................... 25

14. RISK WARNING .............................................................................................................. 26

15. CONCLUSION .................................................................................................................... 27
1. Introduction

1.1 Restructuring the Internet

EON redefines the Internet. EON’s Super Virtual Machine (SVC) is a huge decentralized host. Blockchain technology is just its operating system. The storage of files and logs constitutes its hard drive. And virtual cloud computing serves as its CPU. On the desktop of SVC are various DApps, whose industries involve not only IT, finance, but also all other aspects of society.

1.2 Final generation blockchain

Instead of a fork of EOS, EON is building a more ambitious network based on EOS, which is similar to Telegram Open Network (TON). EOS is just a basic setting for this grand network. As an ambitious project, EON has identified the three most influential and most profitable
companies in the world as the benchmark: Amazon-AWS; Apple Appstore & Iclond; Microsoft Cloud and its development tools.

EON will become a key factor for the Internet to enter the era of value from the era of information. Value Internet is a next-generation network based on cloud computing, blockchain, and big data. EON defines a set of distributed Internet protocols, which breaks through the traditional blockchain thinking and is no longer limited to mere distributed solutions. Starting with the industry infrastructure, the solution provides blockchain, P2P networks, storage, agents, DNS, etc. for users on the entire EON network to decide what they want to do based on what they are good at, their own interests and goals. In this way, the Internet in the Information Age has truly entered the era of value Internet.

• Blockchain service

EON is a flexible cross-chain platform capable of processing millions of transactions per second with intelligent and scalable blockchain scripts. The blockchain exists in the EON network only as a distributed ledger used to save critical data.

• DNS service
EON also provides DNS resolution service that enables accounts, smart contracts, services, and network nodes to provide names routinely recognized by the average user, allowing users to access the Value Internet more easily.

- **Agency service**

An anonymous layer provided by the EON network is mainly used to hide the identity and IP address of the EON network. When a user uses an account containing a large number of cryptocurrencies to conduct transactions, relevant IP, geographic information, and identity information, etc. can be hidden to reduce the risk of DDoS attacks.

- **P2P network service**

It is mainly used to access the EON blockchain, send candidate transactions, and receive updates about the parts of interest to the user. It can support the sending of information in any area.

- **Cloud storage service**

A distributed document storage technology is used by EON blockchain to archive copies of block and state data, which greatly improves storage efficiency through multi-tier cloud storage technology.

## 2. EON Overview

Ancient Greek 'Boule' system is the earliest form of democracy. The Citizen Convention allows any citizen over 20 to participate in the discussion and decision-making of major state issues. Participants receive a small amount of monetary incentives; And the "500 Conference" consists of 500 citizens who have reached the age of 30. Their term of office is one year, and they cannot be re-elected. Each citizen can serve only up to twice in his
lifetime. This system is designed to greatly mobilize participation of each citizen, while taking into account the fairness of the election.

EON’s original Boule algorithm builds on the basis of DPOS, Algorand, Zilliqa and PBFT. It integrates the ideas of sharding from Ethereum Casper and Zilliqa to boost scalability to 10,000 TPS, VRF from Algorand to find the elector nodes, PBFT from Tendermint for quick and safe consensus within each shard. EON also introduces the concept of asynchronous elastic storage, thus solving the need to wait until all other nodes or super-nodes to agree on the data part of blocks. Boule algorithm boasts low latency and high throughput processing capabilities, enabling many more real-world cyber-societal applications experiments. EON blockchain are composed by two types of nodes: 1) addressable nodes (AN) and 2) flexible storage nodes (FSN). Addressable nodes manage the meta information on sharding and routing, while flexible storage nodes stores state transition information.

EON will build a verification & security layer above the smart contract computing layer. EON eWASM VM only supports code written in Coq, F* and Isabelle, which provide data flow programming targeted for 1) parallel computing and map-reduce like sharding optimization; 2) formal verification support. Only programs passing the mathematical proof can be accepted and compiled.

To boost developer friendliness, EON as EOS Network will start as the core network for EOS Developers, which has a smart contract driven code hub and marketplace, targeted for code sharing and exchange. Typically developers can write smart contracts with HTML++ based on available modules and libraries, thus minimizing the chances for developers dealing with VM runtime directly. Thus developers can write smart contracts like build a webpage.
3. Virtual Cloud Computing

3.1 Infinite Decentralization Concept

The number of EOS holders and EOS web developers are both considerable. Although EOS has greatly improved the efficiency of request processing compared to traditional Ethereum, it is still not enough for a large number of decentralized development needs. In particular, blockchain communication speed of EOS is a huge challenge for application developers. EOS has solved many problems of Ethereum, but it is still difficult to create a developer-friendly environment due to the bottleneck of network communication efficiency.

If a main chain is expected to support millions of commercial distributed applications, it must provide extremely high TPS for an instant experience. In order to meet this demand, EON adheres to the idea of infinite decentralization. The nodes served by computers form a public network to provide distributed cloud computing services. Both the deployment of smart contracts and the operation of DApp can be implemented in this cloud.
3.2 Threshold relay

EON uses "threshold relay (TRT)" technology to generate blocks with extremely high efficiency, thereby reducing the processing time of online requests and increasing the response speed. The algorithm generates a random wizard internally, and each newly-created legitimate random array will combine the corresponding miners into a new threshold group. Different threshold groups will not generate any interaction, and they will have independent threshold signatures. When the entire EON network is started, there are several defined threshold groups. The previous group of threshold signatures is used to generate a new random array, and the next-generation threshold group formed by this array will be threshold-signed for the previous random array to legalize it. Through such relays, unlimited distributed random arrays can be generated to achieve the effect of infinite scalability, that is, to realize infinite decentralization.

Threshold relay has obvious advantages over EOS blockchain, mainly because a network can support multiple chains simultaneously without affecting network communication efficiency and security. Each block is also allocated a fixed block time, which provides an incentive system for miners encouraging miners to provide greater support within a limited time.

3.3 Multi-layer cloud

At the same time, EON also uses a block hierarchization technique to divide the consensus mechanism, request processing and data storage into three levels. The request processing and consensus mechanisms do not directly interact with each other. Instead, the storage layer is quantized as a hash unit distributed on all cloud computing nodes. As long as the basic nodes of cloud computing are expanded, the entire data storage scale can grow in synchronization. And these quantized hash storage units are fragmented so there is no need to worry about being consulted by the local node.
4. Super virtual computer

4.1 AI is Law

The natural anonymity of the blockchain has led to a great many hacker attacks on the blockchain for a long time. For example, the Ethereum’s DAO hack reflects typically "Code is Law". Through code loopholes, programmers can get away with stealing tokens worth tens of millions of US dollars. This will be a fatal blow to any commercial application. In order to solve this kind of problem, EON has built a set of EON neural network, which forms a new distributed algorithm by combining human thinking and intellectualized code. EON pursues the "AI is Law" principle and uses EON neural network to establish an algorithmic tribunal, which can perform vetoes and corrections unconditionally for any code operation that is determined to be erroneous.

4.2 SVC Drive Mechanism

The cloud computing system of infinite scalability is also called a super virtual machine (SVC). The EON’s SVC is not a standard artificial intelligence, but it simulates the information process of human consciousness and thinking in artificial intelligence. The artificial consciousness of the administrator exerts intelligent awareness on the entire SVC. SVC uses the computers of excellent nodes to build local neurons. All local neurons form the
EON neural network together to make decisions on the requests provided by local neurons. SVC handles problems through an indeterminate distributed algorithm, and it continuously improves its ability to submit proposals through a loop feedback learning mechanism.

All users in the EON ecosystem only need to pay the corresponding Token deposit to become a local neuron and participate in the SVC's neural network decision-making. SVC provides a set of non-public voting mechanism, in order to protect the rights of each local neuron and prevent blind votes, thus making the election results more fair and balanced. The voting weight of each neuron is directly proportional to the amount of deposit it pays. After creating the neuron and paying the corresponding deposit fee, the client will receive the installation key so that the local neuron can receive various proposals requested by SVC.

All local neurons can vote through their managers. If managers do not vote before the corresponding time node, neurons automatically follow the selection results of other neurons that are closest to their own attributes. If managers do not want this to happen, they can establish a corresponding long-term algorithm to supervise their voting.

### 4.3 Multilayer Neural Networks

In order to achieve a good effect of neuron supervision and management, EON neural network adopts the structure of multilayer sensor. A general multilayer neural network is a directed graph of a forward structure. It is composed of multiple local neuronal layers. Each layer is connected to the next layer. Except for input nodes, each neuron is a processing unit with a nonlinear activation function. Such an approach avoids the inability of a single neural network to classify data for identification and enhances the large-scale processing capabilities of the virtual cloud.

And training multi-layer neural networks will inevitably involve many different problem algorithms in order to continuously optimize this governance algorithm. Therefore EON adopts the most popular back propagation algorithm and generalized incremental rules to optimize it. The back propagation algorithm requires that the multilayer neural networks should be composed of at least three layers: the input layer, the hidden layer, and the output layer. The units in each layer are connected to all the units in the adjacent layer, and there
is no connection between the units in the same layer. After providing a pair of learning samples to the EON network, the activation values of the neurons propagate from the input layer through the middle layer to the output layer, and the input responses of the network are transmitted to each neuron in the output layer. Next, in order to reduce the error in the output direction of the target, each connection weight value is corrected layer by layer from the output layer through each intermediate layer, and finally returned to the input layer.

One of the biggest problems faced by neural networks is how to choose the right structure network. This is especially important in unknown environments. EON tries to find a way to change the structure of neural networks. That is, if during the optimization training, the error has stabilized but is larger than our target error, we will generate a new hidden layer neuron. When the neuron is no longer a functional element of the EON network, it can be eliminated unconditionally. If the neuron is a redundant element but can guarantee a constant output, it will establish a connection with another neuron. These criteria in the same layer can be checked by monitoring the input weight vectors of the neurons. If two of them are linearly related, they will manifest the same Hyper Plane in the spanning data space and be completely interdependent. If the output is a constant value, the output entropy is approximately zero. This method is useful for finding the optimal design of a neural network without demand of extensive domain knowledge.

5. Consensus Layer

Overview

In EON's blockchain structure, nodes are classified as "addressable nodes" and "elastic storage nodes". The initial EON node will be divided into 160, and will continue to increase as the number of nodes increases. There is an upper limit for each node's addressing (currently 100), and each one is
called an shard. Each node has the qualification to obtain the addressed node in its area. The probability is directly proportional to its total coin age ($\sum_a$) and satisfies:

$$\sum_A = \sum_i A_i \cdot T_i$$

where $A_i$ is total balance of individual UTXO and $T_i$ is its length of its holding time.

The election will use Algorand algorithm [2]. The node calculates the Verifiable Random Functions (VRF) and knows whether it is selected as an addressable node. Simply put, for any node that holds a public and private key pair ($P_K$, $P_V$), two values are returned: the hash value and the proof value, the hash value is uniquely determined by the input string (the block hash), and the proof value allows anyone to check the hash is valid. Based on this zero-knowledge proof, entire network can quickly identify random electors and achieve consensus using the PBFT algorithm.

![Figure 3.1: EON Blockchain Structure](image)

The number $N$ of values randomly calculated by the addressed node in EON's elastic accounting node during the operation process is a variable that needs to be constrained. The $N$ value exceeding the conference sacrifices the operating efficiency of the EON blockchain. Before the node joins the new slice area, therefore, as the number of nodes in the EON community (assumed as $S$) increases, until the final $N$ converges. We have $N < S$ and $dN/dt \ll dS/dt$. 
Cryptography

EON uses SHA-3 [Dworkin_2015] hash function for common tasks other than digital signing. Each of the SHA-3 functions is based on an instance of the KECCAK algorithm.

EON uses Elliptic Curve Based Schnorr Signature Algorithm (EC-Schnorr) as the base signing algorithm. EON instantiate the scheme with secp256k1 curve. The same curve is currently used in Bitcoin and Ethereum but for a different signing algorithm called ECDSA. Choosing ECSchnorr over ECDSA has several benefits that we discuss below:

- **Non-malleability**: Informally put, the non-malleability property means that given a set of signatures generated on a message using a private key, it should be hard for an adversary to produce a new signature for the same message that is valid for the corresponding public key. Unlike ECDSA which is malleable, EC-Schnorr has been proven to be non-malleable.

- **Multi-signature**: A multi-signature scheme allows multiple signers to “aggregate” their signatures on a given message into a single signature which can be authenticated against a single public key that “aggregates” the keys of all the authorized parties. While, EC-Schnorr is natively a multi-signature scheme, ECDSA allows creating multi-signatures but in a less flexible way.

- **Speed**: EC-Schnorr is faster than ECDSA since the latter requires computing an inverse modulo a large number. No inversion is required in EC-Schnorr.

- **Verifiable Random Function**
A Verifiable Random Function (VRF) is the public-key version of keyed cryptographic hash. Only the holder of the VRF secret key can compute the hash, but anyone with the public key can verify the correctness of the hash.

A VRF comes with a key generation algorithm that generates a public VRF key $P_k$ and private VRF key $S_k$. A VRF hashes an input $\alpha$ using the private VRF key $S_k$ to obtain a VRF hash output $\beta$:

\[
\beta = VRF_{\text{hash}}(S_k, \alpha)
\]

The VRF$_{\text{hash}}$ algorithm is deterministic, in the sense that it always produces the same output $\beta$ given a pair of inputs $(S_k, \alpha)$. The private key $S_k$ is also used to construct a proof $\pi$ that $\beta$ is the correct hash output:

\[
\pi = VRF_{\text{prove}}(S_k, \alpha)
\]

The VRFs defined in this document allow anyone to deterministically obtain the VRF hash output $\beta$ directly from the proof value $\pi$ as

\[
\beta = VRF_{\text{proof2hash}}(\pi)
\]

Notice that this means that

\[
VRF_{\text{hash}}(S_k, \alpha) = VRF_{\text{proof2hash}}(VRF_{\text{proof}}(S_k, \alpha))
\]

The proof $\pi$ allows a Verifier holding the public key $P_k$ to verify that $\beta$ is the correct VRF hash of input $\alpha$ under key $P_k$. Thus, the VRF also comes with an
algorithm

\[ VRF_{\text{verify}}(P_k, \alpha, \pi) \]

that outputs VALID if \( \beta = VRF_{\text{proof2hash}}(\pi) \) is correct VRF hash of \( \alpha \) under key \( P_k \), and outputs INVALID otherwise.

EON use of VRFs to randomly select elector nodes within each shard in a private and non-interactive way [Micali_1999]. Using VRFs, EON implements node election (a.k.a cryptographic sortition) as shown in Algorithm 1.

```
Data: sk, seed, τ, role, w, W
Result: Select random elector nodes who participate the PBFT consensus process

initialization;
<hash, π> ← VRFsk(seed||role)
p ← \frac{τ}{W}
j ← 0
while not at end of this document do
    j++;
end
```

- PBFT (Practical Byzantine Fault Tolerance) algorithm

- The consensus between elective nodes within shards rely on practical byzantine fault tolerance (PBFT) protocol. We improve its efficiency by using the idea of employing EC-Schnorr multisignature in the PBFT protocol as developed in [Micali_1999], [DBLP:journals/corr/Kokoris-Kogias16]. Use of EC-Schnorr multisignature lowers the normal case communication latency from \( O(n^2) \) to \( O(n) \) and reduces the signature size from \( O(n) \) to \( O(1) \), where \( n \) is the size of the consensus group. In this section, we present an overview of PBFT. In PBFT, all the nodes within a consensus group are ordered in a sequence, and it has one primary node (or leader) and the others are referred to as backup nodes.

- A client multitasks a request to all server replicas. A request has the form \(<request, o, t, c> \sigma_c\), where \( o \) is the operation to be executed at the server.
replica, $t$ is a timestamp, $c$ is the identifier of the client, and $\sigma_c$ is the client’s digital signature for the request. The client must ensure that a later request bears a larger timestamp. The timestamp $t$ is used by the replicas to detect duplicates. If a duplicate request is detected, the replica would return the logged reply to the client instead of reordering them.

- The server replicas exchange control messages to establish and agree on the total order for the request. The complexity of the PBFT algorithm lies in this step.

- The server replicas execute the request according to the total order established and send the corresponding reply to the client. A replica may have to delay the execution of the request until all requests that are ordered ahead of the request have been executed.

- The client would not accept a reply until it has collected consistent replies to its request from $f + 1$ server replicas. This is to ensure that at least one of them comes from a non-faulty replica. A reply has the form $<\text{reply}, v, t, c, i, r > \sigma_i$, where $v$ is the current view number, $t$ is the timestamp of the corresponding request, $i$ is the replica identifier, and $r$ is the application response as the result of the execution of the operation $o$. The client verifies consistency by comparing the $r$ component in the reply message.

Classical PBFT uses message authentication code (MAC) for authenticated communication between nodes. As MAC requires a secret key shared between every two nodes, the nodes in one consensus group can agree on the same record with a communication complexity of $O(n^2)$ per node. Due to the quadratic complexity, PBFT becomes impractical when the committee has over 20 nodes. To improve the efficiency, we use the ideas inspired from ByzCoin [DBLP:journals/corr/Kokoris-KogiasJ16]. We replace MAC with digital signatures to effectively reduce the communication overhead to $O(n)$. 2) In the meantime, to allow the other nodes to verify the agreement, one typical way is to collect the signatures from the honest majority and append them to the agreement, thereby resulting in the agreement size...
linear in the size of the consensus group. To improve on this, we employ EC-Schnorr multi-signatures to aggregate several signatures into an $O(1) - size$ multi-signature.

6. Smart Contract Protocol Layer

- State

As in Ethereum and Ziliqua, there are two types of accounts: normal account and smart contract account. A normal account is created by generating an EC-Schnorr private and public key pair. Smart contract accounts are created by normal accounts.

The addresses of normal accounts are defined in the same way as Ethereum. The address of the new account is defined as being the rightmost 160 bits of the SHA-3 256 hash of the RLP encoding of the structure containing only the sender and the account nonce. As such the account address $\alpha$ is:

$$a \equiv B_{96,255}(SHA3(\text{RLP}(<S, \sigma[s]_n - 1>)))$$

where SHA3 is Keccak 256-bit hash function, RLP is the RLP encoding function as defined in [Wood_2018], $B_{a,b}(X)$ evaluates to a binary value containing the bits of indices in the range $[a, b]$ of the binary data $X$, and $\sigma[x]$ is the address state of $x$, or $\emptyset$ (an empty string) if none exists. The nonce value $s$ evaluated as the number of transactions sent from a normal account. In case of a contract account, it counts the number of contract creations made by the account.

Each account is associated with an account state. The account state is a in memory key-value store (typically redis, zeromq and rabbitmq), typically composed with the following keys. Since the definition would be mostly identical with Ethereum, we use the same symbol sets for the same meaning as [Wood_2018], if not otherwise specified.
The global state (state) $\Sigma$ is a mapping between account addresses and account states. It is implemented using a trie like data structure. Global state is not stored but inferred [Wood_2018], only the root hash is stored in block head.

- Transaction There are two types of transactions: those which sending message (function calls) and those which result in the creation of new accounts with associated smart contract code. We follow the same symbol set as Ethereum if not otherwise specified.

$\beta_{\ldots\infty}$ means an expandable byte array that specifies the contract code, present only when the transaction creates a new contract. $D$ specifies the data that should be used
to process the transaction, present only when the transaction invokes message calls.

\( P_k \) is an EC-Schnorr public key that should be used to verify the signature. The pubkey field also determines the sending address of the transaction. \( ES_s \) is an EC-Schnorr signature on the entire data.

- Blocks In the block structure, EON adopts Ethereum and Zilliqa except the POW part.

<table>
<thead>
<tr>
<th>parentHash</th>
<th>ownersHash</th>
<th>beneficiary</th>
<th>stateRoot</th>
<th>transactionsRoot</th>
<th>receiptsRoot</th>
<th>logsBloom</th>
</tr>
</thead>
<tbody>
<tr>
<td>( H_p )</td>
<td>( H_o )</td>
<td>( H_c )</td>
<td>( H_r )</td>
<td>( H_t )</td>
<td>( H_e )</td>
<td>( H_0 )</td>
</tr>
<tr>
<td>number</td>
<td>gas limit</td>
<td>gas used</td>
<td>timestamp</td>
<td>extra data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>( H_t )</td>
<td>( H_l )</td>
<td>( H_a )</td>
<td>( H_s )</td>
<td>( H_x )</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A DS-Block has the following unique fields:

\[ ES_s \]

\[ B \]

Blocks have two types: transaction blocks (TX-Block) and directory service blocks (DS-Block).

\( ES_s \) is an EC-Schnorr based multi-signature on the DS-Block header signed by nodes within the same shard. \( B \) records which nodes participated in the multi-signature.

7. Security & Application Layer

Current mainstream blockchain can only perform IO on its own public ledger. EON is essentially a basic public blockchain infrastructure, supporting the establishment of sub-chains and side chains based on different industries, regions, and application scenarios. The blockchain communicates to meet the needs of different scenarios. At the same time, common protocol support for data exchange can be performed between those chains so as to achieve interaction and communication requirements. The final EON blockchain will be presented in a matrix-like three-dimensional network structure, which we will define as EON hyper-network. At the application level, developers can only use F*, Coq, and Isabelle to develop EON’s smart contracts. After the code is formalized and verified, the EON security & virtual layer cross-compiler automatically generates the underlying C++ code to
ensure efficiency and security, as well as minimize possible design flaws. The following is a Ballot smart contract snippet written by Coq:

Record Ballot := create_Ballot {
  voteCounts: IntMap.t (Z);
  delegations: IntMap.t (Z);
  votes: IntMap.t (Z);
  voted: IntMap.t (bool);
  voterWeight: IntMap.t (Z);
  numProposals: Z;
  chairperson: Z;
}.

Definition get_voteCounts (mapping : IntMap.t (Z)) (a0 : Z) :=
let m1 := match (IntMap.find a0 mapping) with
  | None => 0
  | Some a => a end in
  m1.

The formal verification development language is very difficult for non-mathematics major developers. To reduce the development threshold, EON provides:

- The HTML++ language is an extension of HTML. It can be cross-compiled into Coq code in the security and privacy layer, and the relevant tags of the blockchain are increased. The pre-compiled smart contract module can be directly used to compose web pages, and the development is fast and secure. With the introduction of smart contract templates, new tags and attributes can be used for rapid development with simple markup languages. The code to implement a future product linked to bitcoin for a decentralized exchange in HTML++ is as follows:
EON public chain embeds cross-chain functions including smart contract interpreter and runtime based on Rootstock and Polkadot, integrated well with Bitcoin and Ethereum.

The EON community will also work with partners to build an open source smart contract template library and online market DApp Store. Developers can share the formalized and compiled code and receive token rewards. The EON community will also provide users with social distribution incentives. Users can use the online IDE Wisdom Studio provided by EON to quickly build smart contracts through familiar controls and event triggering methods and HTML++ syntax.

The above aspects comprehensively form the security verification layer of the EON public chain, providing a safe, efficient, developer-friendly bottom layer, combined with an efficient settlement consensus, will fundamentally solve the current major problems of current mainstream blockchain technology.

8. EOS landing platform

EON makes the whole ecology of EOS come true, and revolutionizes use cases. EON replaces the single node of EOS with a cluster/multi-chain/sharding approach to achieve millions of TPS.

As the most influential EOS implementation platform, we will promote the large-scale
application of EOS in the following three ways.

- EON will become the first cloud computing platform for EOS. EOS/EON can be used to purchase cloud computing, storage, bandwidth, DNS and other services;
- EOS can be used to purchase various DApps in the App Store;
- Developers can use EOS to purchase smart contracts (dapp source code).

At the same time, in the ecological cycle, block producers and ordinary users can use idle computing power, storage or bandwidth resources to obtain EON. Developers can get EOS/EON by developing DApps or smart contracts.

**9. Token Economics System and Incentivization**

The token is mostly used as gas for elector incentive. Every computation that occurs as a result of a transaction on the EON network incurs a fee. This fee is paid in a denomination called “gas.” Gas is the unit used to measure the fees required for a particular computation. Gas price is the amount of EON you are willing to spend on every unit of gas. With every transaction, a sender sets a gas limit and gas price. The product of gas price and gas limit represents the maximum amount of Wei that the sender is willing to pay for executing a transaction.

When developers submit a compiled library/module or DApp on EON Security Layer and Application Layer, they are required to pay a certain gas to avoid spamming. At the same time, the EON tokens are used for making purchases.

**10. Community & Platform Features**

- Wallet/browser EON community combines the browser and wallet together to facilitate the integration with blockchain. The sandbox model are applied to
effectively separate different levels of private keys.

- EON employs a first of its kind hierarchical private key system to facilitate low-security and high-security transactions. Low-security transactions tend to be social, such as posting or commenting. High-security transactions tend to be transfers and key changes. This allows users to implement different levels of security for their keys, depending on the access that the keys allow.

### 11. Roadmap

![Roadmap Diagram]

### 12. Token Allocation

**Airdrop policy**

In order to realize the ecological balance of EON as early as possible, EON conducted a large-scale airdrop at the initial stage. The total number of airdrops accounts for 90% (current scale of 900 million EON) of EON tokens. Since many members of the EON community are also EOS's outstanding contributors, after months of lengthy discussions we decided to conduct a 1:1 directional airdrop to EOS holders in order to allow them to establish a common ideal with us and promote the entire EON ecological development.

**Reserve policy**
EON is a long-term project, and we firmly believe it. For this reason, we lock 10% (100 million EON) of the tokens held by the team. The lock-up period is 48 months. After that, it will be unlocked by 12.5% every 6 months. This means that the founder can't trade tokens immediately, thus ensuring that the founding team can focus on the long-term development and benefits of the project.

**Block Producer Award**

As the main node that sustains the entire ecosystem of EON, they continue to create value for EON. In this regard, we will issue additional 5% tokens each year as a reward for the nodes and issue it to those who maintain the main nodes.

**The tokens are allocated as follows:**

Total amount of tokens 1 billion with 5% annual inflation.

Airdrop: 90%

Team: 10%

---

**EON Token Distribution**

- **Airdrop**: 90%
- **Team**: 10%
Inflation plan after the launch of mainnet:

Inflation of 1 billion tokens will be shared by the team.

Inflation of 1 billion tokens will be shared by investors.

Increased shares for team and investors will be locked for 48 months, then unlocked by 12.5% every 6 months.

At the same time the mining pool is open. Mining will increase up to 7 billion tokens, of which miners will receive 80% (5.6 billion) for rewards and additional revenue for block producers accounts for 20% (1.4 billion).

13. Team

Orc Guo

Guo has more than 15 years of work experience in Silicon Valley high-technology companies, a financial consulting agency and a VC. He previously worked as a consultant and senior executive for globally renowned companies including KPMG, World Bank, Apple, and LinkedIn. He established two blockchain startups in Silicon Valley and successfully exited. Guo graduated from Carnegie Mellon University majoring in Electrical and Computer Engineering, where he won the Conrad scholarship.

Yeh T'ien

Dr. T’ien is an artificial intelligence expert and formerly was a distributed computing researcher of Google Inc.. With a Ph.D. from Virginia Tech and a bachelor's degree from Tsinghua University, he has profound understanding and experience in the integration of artificial intelligence and blockchain industry.
14. Risk Warning

Policy risks

Although most governments currently have a clear-cut and positively encouraged policy toward blockchain-related industries, the decentralized nature of the blockchain itself still poses many uncertain risks under existing government-centric laws and regulations. In response to this type of risk, the EON team will actively maintain communication and collaboration with relevant organizations and conduct blockchain application related business under the legal framework.

Market risk

As the blockchain industry has just emerged, it will face multiple challenges from traditional industries. In response to market risks, the EON team will actively communicate with community practitioners on a regular basis, collaborate effectively, and strive to adapt to the needs of the market. It will not hold regular conferences to ensure the project can face the needs of the market.

Capital risk

Here mainly refers to the occurrence of serious human-induced loss of project funds due to certain circumstances. In order to avoid such risks, EON team funds will adopt multi-signature methods to reduce the probability of man-made losses.

Technical risk

Since EON will establish a multi-chain network with EOS as its main body, the technical challenges facing it are unprecedented. This is a very high requirement for the technical and talented personnel and the degree of concentration. If we cannot consistently overcome the technical difficulties, It is very likely that delaying the project will even result in the project eventually failing. In response to such risks, the EON team will strengthen cooperation with
internationally renowned universities and blockchain giants and try their best to ensure the controllability of technology risks.

15. Conclusion

In this whitepaper, we have presented EON’s hierarchical architecture that allows blockchain network to process transactions in parallel and securely. EON comes with a unique smart contract IDE that leverages formal verification for maximum security. To enhance developer friendliness, EON provides a code hub and marketplace where developer can find precompile libraries scanned and checked by entrusted third parties. Based on the modules, developers can write smart contracts in HTML++, a very familiar way with a common webpage.
References