EtherZero

THE FUTURE OF SMART CONTRACT PLATFORM & DECENTRALIZED APPLICATIONS BLOCKCHAIN

EtherZero White Paper
Revision:2

Etherzero

Smart Contract Platform & Decentralized Applications Blockchain

EXECUTIVE SUMMARY

This document describes EtherZero or ETZ as the evolving platform for the implementation of a general smart contract development, with 0 transaction fees, high transaction processing capacity, near real-time transactions.

By utilizing ETZ platform, developers can build more general-purpose decentralized applications, these applications can revolutionize current narrow scope of financial and commercial applications, ETZ can help blockchain and decentralized-services to reach a wider range of people and services, ETZ will change blockchain application industries.

EtherZero extends the Gas mechanism of Ethereum, and extends the concept of Power on the basis of it, giving each account access to network resources that are positively correlated with the amount of coin it holds, and the speed of reply when such access is used. Thus, the characteristics of zero transaction fee are carried out safely through mitigating possible attacks or hacks.

Based on the knowledge of Masternode and PoW double-layer network and distributed autonomous architecture nature of DASH Coin and Clique protocol from Ethereum's Proof of Authority Rinkeby testnet, an EtherZero consensus algorithm called MPoS (Masternode + PoS) is designed and implemented.

This consensus algorithm enables standard transaction exchanges between accounts as well as empowering the community with autonomy to run masternodes. A pre-requisite to be a masternode participant is to hold an agreed amount of EtherZero coins and running it on a performance-compliant hosted server. Currently, based on network parameters such as MPoS consensus and properly set out block time, EtherZero can achieve a high degree of decentralization with a high number of masternodes and with transaction processing capabilities of above 1400 TPS.

Etherzero

Smart Contract Platform & Decentralized Applications Blockchain

TABLE OF CONTENT

Etherzero

Smart Contract Platform & Decentralized Applications Blockchain

1. INTRODUCTION TO ETHERZERO

EtherZero (**ETZ**) is a new generation of smart contract platform initiated by a group of professional and technical geeks worldwide to provide better service to DAPP developers and users. ETZ Team is aware of the needs to always maintain the platform to thrive the challenge for the needs of high-quality requirement including security.

Recently, ETZ announced the ETHERZERO 2.0 Version. ETZ's latest improvement has been successfully achieve its goal to provide thousands of TPS smart contract blockchain and using revolutionary zero-fee under current new version platform.

Don't forget that ETZ is always evolving, ETZ always improves to cope the blockchain platform and its application needs.

1.1 BACKGROUND

EtherZero or abbreviated as ETZ is a General Smart Contract Development Platform and it has unique features as a smart contract capability with 0 transaction fees, high transaction processing capacity, near real-time transactions.

ETZ was built based on the knowledge of Masternode + PoW double-layer network and distributed autonomous architecture nature of DASH[1] Coin and Clique protocol from Ethereum's Proof of Authority[2] Rinkeby testnet.

ETZ is a growing and innovative platform, one should expect that ETZ will always be configured to answer the demand to serve multi smart contract and other blockchain needs. Currently ETZ is arranged under a new and better consensus under the new version leaving its previous PoW and its Masternode mechanism to a new configuration using MPoS.

What are the advantages of the latest EtherZero Version or ETHERZERO 2.0 ?

Current ETHERZERO (or ETHERZERO 2.0) is a double-layer network structure which is better than previous double layer network of ETHERZERO Version 1.0 which use a Masternode and PoW two-layer concensus. ETZ Team found from other network hacking attacks that PoW based platform is likely to be more susceptible compare to full PoS mechanism.

[1] Dash.org - https://docs.dash.org/en/latest/introduction/about.html#whitepaper

[2] The Ethereum Proof-of-Authority protocol is called Clique and is well described in the Clique Github issue. Ethereum currently uses this algorithm for the Rinkeby test network. Ethereum core developer, Peter Szilagyi https://github.com/ethereum/EIPs/issues/225

• New consensus mechanism MPoS replaces the initial design of the Masternode + POW two-layer network consensus;

• After deleted the double-layer network, the masternode has full authority to handle all transaction verification and packing block work;

• Detailed design and implementation of the Power mechanism to support dynamic network resource configuration;

• Detailed design and implementation of a community governance framework based on masternodes and smart contracts;

• MPoS consensus will affect the underlying economic mechanism, 75% out of the rewards is for masternode, and the rest is for community budget;

• The MPoS consensus-based main network is online and needs to plan the next task.

1.2 DEFINITION

Blockchain	:	A digital ledger in which transactions made in bitcoin or another cryptocurrency are recorded chronologically and publicly.
Bitcoin	:	A type of digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank.
BTC	:	Bitcoin.
DASH or Dash or DASH Coin	:	A peer-to-peer cryptocurrency that was forked out of Bitcoin to offer faster and more private transactions to users. Dash is the first digital currency with a decentralized blockchain governance system using Masternode Mechanism in a combination with PoW consensus.
DDoS Attack	:	Distributed Denial-of-Service Attacks
ETH	:	Ethereum
ETZ	:	EtherZero
EtherZero	:	General smart contract development platform, with 0 transaction fees, high transaction processing capacity, near real-time transactions.
MN	:	Masternode
MPoS	:	Masternode Proof of Stake

MPoW	:	Masternode Proof of Work
PoS	:	Proof of Stake
PoW	:	Proof of Work
TPS	:	Transaction per Second

1.3 MARKET CONDITIONS

Eventhough at the end of 2017, the encrypted digital currency, also known as cryptocurrency, already has a total market capitalization exceeding 600 billion US dollars and be likely still increasing, but it is undeniable that most of investors don't really understand about cryptocurrency, and also confused about how blockchain can achieve trustworthy transaction value, and it is even more absurd to discuss this with outsiders – common peoples who knows nothing. While some peoples started to recognize cryptocurrency or blockchain in 2018, the overall cumulative market caplitalization seems to increase over next year[3].

In order to speed up mass adoption, public should be familiar with blockchain. This also means blockchain and cryptocurrency urgently need killer application which can help common peoples to understand more about cryptocurrency and blockchain technology which will give big impacts to their lives. This kind of killer application is not exist independently, but should be built on a public chain smart contract development platform which support some of key characteristics. EtherZero is built based on these considerations.

It still needs more effort for blockchain and cryptocurrency enthusiasts around the world before mass adoption ready, the key to mass adoption is to make every blockchain and cryptocurrency application simple and easily use by everyone.

Mass adoption also means that we are in urgent-need of a class of killer platform and applications that can help more ordinary peoples to understand the tremendous impact of the technology of blockchain and cryptocurrency on their daily lives.

This kind of killer applications do not exist independently but rather should be built on a public chain that supports some of the key features with smart contract development platform. EtherZero is based on this assumption.

[3] Global Cryptocurrency Benchmarking Study, Dr Garrick Hileman & Michel Rauchs 2017, University of Cambridge Judge Business School, p15

EtherZero is made for any possible application to be featured with blockchain technology and EtherZero is positioned itself as the one who combine, promote blockchain technology and make it popular for daily use.

The reason why we need to combine it is because the fact that most of today's innovative blockchain technologies are still in the experimental stage, severely isolated from one another, and applied in the field that are not clearly defined. It needs an organization to stand from the spectator point of view to observe the possibilities to integrate application of these technologies and provide developers with an operating system which can accommodate various technologies and is oriented to the application.

After completing masternode development, EtherZero will use private placement funds to recruit new blockchain technical staff to integrate the existing technologies which in the long run will promote transformation of technologies into practical application by using production and experimental network in parallel. Promoting and making the blockchain technology popular for daily use are targeted on real application scenarios. A technology must have real usability scenarios and create economic benefit breakthrough to the existing technology system in order to become mainstream. We will organize one specialized Industry Application Working Group with team members from conservative industry experts, blockchain technicians, and blockchain developers.

Extensively, we also conduct industrial research and scenario feasibility studies on various industries in the current society, with a hope to successfully deepen and popularized blockchain revolution.

Blockchain developers are currently offering so many types and concepts of its technology. These various technology-schemes may also mean that it will become a big obstacle in the process for normal user to understand and enjoy blockchains. we want to avoid users to directly contact the complex concept through a combination of cognition and technology, and exporting a mature product to users. We will do our best to guide community developers to develop real and reachable products.

1.4 GENERAL APPLICATION PLATFORM REQUIREMENTS

ETZ is made to accommodate any application, we believe that ETZ can host multiple killer platform and this killer application can only be built on such a features on ETZ:

Basic Operations with Zero Transaction Fees: In order to support the development and business operations of decentralized applications in a broader sense, various basic operations, such as registration, login, collection, browsing, search, sharing and various small/negligible services or operations should not be charged. ETZ can provide every possible service without fee.

Super-high concurrency and scalability: The ability to operate concurrently with the contract code on block chains for users worldwide, data concurrency is a challenging issue to tackle, so this kind of application platform have enough scalability to be able to expand proportionally along with the growth of users and applications.

Real-time feedback: The vast majority of the user's operations should have real-time feedback under secure condition. It is the basic requirement for decentralized application to be comparable with traditional applications.

Version system: Application version system helps developers to quickly complete bug fixes, and for developers to conveniently complete A/B testing for user studies.

Platform Evolution: Community Proposal Systems and Masternode Voting can help to drive community-driven evolution of EtherZero. It facilitates the rapid implementation of various technical iterations and platform governance rules.

The Most Critical Component Functions: Decentralized storage such as IPFS protocol, secure hotfix procedures, and the underlying platform services for identity authentication, anonymous communication, notification systems, etc.

1.5 ETHERZERO KEY FEATURES

Zero transaction fee

EtherZero extends the Gas mechanism of Ethereum, and improves the Power mechanism on the basis of it. It gives each account the right to use network resources. It also governs the speed of transaction response when the right is used. Thus, the characteristics of zero transaction fee are carried out safely. The transaction initiator only needs to hold and the transaction does not need to consume the basic currency of the network (zero fee).

Fast Confirmation

In the new EtherZero network, the trade side can define the number of verification blocks required for transaction confirmation by themselves. Since the outgoing time is shortened to 1s and the number of masternodes authorized to generate block in the cycle is 21, therefore even considering security, all transactions can usually obtain more than 99% confirmation within 3s, and the final transaction

confirmation within a maximum of only 15s. The confirmation/verification is very fast especially if it is compared with current available blockchain technology as it may need couple minutes to hours duration.

High throughput

Based on the MPoS consensus, and setting the appropriate time to generate block and other parameters, EtherZero has implemented more than 1400 TPS transaction processing capabilities on thousands of masternode structures.

Open decentralized community autonomy

EtherZero built the MPoS (Masternode+PoS) consensus mechanism on the basis of DASH Coin's Masternode + Pow double-layer network and community autonomy structures and Clique consensus algorithm of ETH. In this consensus mechanism, anyone can participate in EtherZero network transaction processing and community autonomy after hold an agreed amount of EtherZero coins and build server that meet requirements.

At the same time, since 21 masternodes are selected from thousands of masternodes in each approximately one hour voting cycle, this provides a super-high degree of open decentralization.

Proposal decision and budget distribution functions based on voters in the masternode have been developed and integrated into the EtherZero master network.

2. ZERO TRANSACTION FEE INTELLIGENT CONTRACT DEVELOPMENT PLATFORM

Zero transaction fee is revolutionary and it can make any small blockchain can be rolled to be a real blockchain services in many possible applications.

2.1 NECESITY OF ZERO TRANSACTION FEE

The most persuasive tool of EtherZero characteristics is zero-transaction fee.

Taking the simplest distributed collaborative to-do list, or to-do application, as an example, its decentralized implementation can be applied to the task decomposition process of a global decentralized collaborative team. This process requires each participant in the project to understand the tasks of other unfamiliar members. Everyone's task is validated by team consensus result, has a certain traceability and need for trust.

We can imagine if we tie a small application on the blockchain on current available concept. Every small steps or service will have cost.

The application involves the registration of members, the addition and deletion of tasks, and so on. According to the operation-requirements on ETH, all these operations require gas consumption or fee. It also means that every service will be eventually converted into ETH and it ll charge to users, which is not reasonable for the small service/operation to be charged with cost (under fee mechanism), it is not economically-wise both for user experience.

In EtherZero, the frequency of transaction initiation and the number of execution steps of intelligent contracts are positively correlated with the balance held in the account. This not only to meet zero transaction cost, but this also takes into account the reasonable use of network resources, and limits the malicious attackers to launch DDoS attacks requiring higher capital investment. This concept of zero transaction cost from an economic perspective will really lead to decentralized applications into the daily-life scene.

2.2 GAS MECHANISM

ETZ has different approaches in gas mechanism. In Ethereum, the transaction fee is calculated by the value of the Ethers, the mining reward, gas incurred and the gas price[4], the gas paid by the initiator of the transaction will eventually be counted at the value of the ETH currency and paid to the miner as a fee, i.e. Gas cost = Gas Used * Gas Price.

The function of Gas and ETH in Ethereum are described as follows:

- A tool to measure computational resources usage in the network;
- Converted into transaction fee, as reward for miner and block verification;
- Converted into transaction fee, as an economical method to resist DoS attacks

In EtherZero, Gas is still used as a computational resources measurement tool and the-fee is replaced and expanded by the Power mechanism.

The Gas and Power mechanisms together established a solid foundation for zero-transaction cost safely.

2.3 POWER MECHANISM

Power is actually a currency which issued for users who hold ETZs, cannot be traded and can only be consumed, representing the power to use network resources (computing, storage, bandwidth, etc.).

[4] Gas Price (Ethereum) - https://www.investopedia.com/terms/g/gas-price-ethereum.asp

Each time you hold an ETZ, you will be distributed a certain amount of Power, and each Power represents 1 share of network resources.

In other words, the zero transaction cost does not mean that the network can be used without any cost, and the user still has to pay the time cost of holding the priceable currency ETZ.

The more the number of coins held by the user, the more power there is, so the network resources that can be used, such as the maximum Power value consumed per transaction, and the recovery rate after Power is consumed.

We can imagine the usability of power on ETZ like a game. In a game, the power value determines the maximum blood volume and blood volume recovery speed.

When a player plays against a monster, it must consume a certain amount of blood to kill a certain monster. The blood consumed should be higher if the monster is more powerful.

For the Power mechanism, the number of ETZ held by user is the power value. The maximum blood volume is the Power Max of the account. The blood recovery rate is Power Speed. The task of killing different types of monsters is to perform different types of operations such as trading or deploying contracts.

Power is different from Gas in ETH:

- For each account, the maximum power is fixed when the account balance is fixed;
- Power can be restored, and the recovery speed is positively related to the number of ETZ coins of the account;
- Power consumption is a power reduction process, but in ETH, calculating the fee through Gas is an accumulation process.

The operation of consuming Power in EtherZero is similar to the type of operation that consumes Gas in ETH:

- Sending a transaction requires an account to consume Power;
- The larger the amount of Data carried during the transaction, the more Power is consumed;
- The more complex calculation of the data in the contract, the more Power is consumed;
- The order in the transaction pool is sorted by Gas Price from high to low.

2.4 MATHEMATICAL EXPLANATION OF POWER

All accounts with a balance greater than or equal to 0.01 ETZ will continue to produce Power as the block grows until the power limit for this account is reached.

Query your own available Power in the Console:

- ✓ eth.getPower("your address")
- ✓ web3.fromWei(eth.getPower("your address"), "ether")

```
Welcome to the Geth JavaScript console!

instance: Geth/v1.8.12-unstable-526ebeac/linux-amd64/go1.10.1
 modules: admin:1.0 debug:1.0 devote:1.0 eth:1.0 masternode:1.0 miner:1.0 net:1.0 per

> eth.getPower("0xdd5b67E58B3A0ad20757c10Cee9B0e33331eaAfd")
3600000000000000
> web3.fromWei(eth.getPower("0xdd5b67E58B3A0ad20757c10Cee9B0e33331eaAfd"), "ether")
0.0036
```

2.4.1 TWO PROPERTIES OF POWER

There are two properties of power in ETZ:

- Upper limit Max value (the upper limit is determined by the ETZ balance);
- Speed of output per block (determined by the ETZ balance);

Power value of an account is calculated as:

Power = Min(PowerMax, BlockGap * PowerSpeed)

BlockGap = current block height – the height of a trading block on this account

Power consumed by a transaction is calculated as:

PowerSpend = Gas * GasPrice

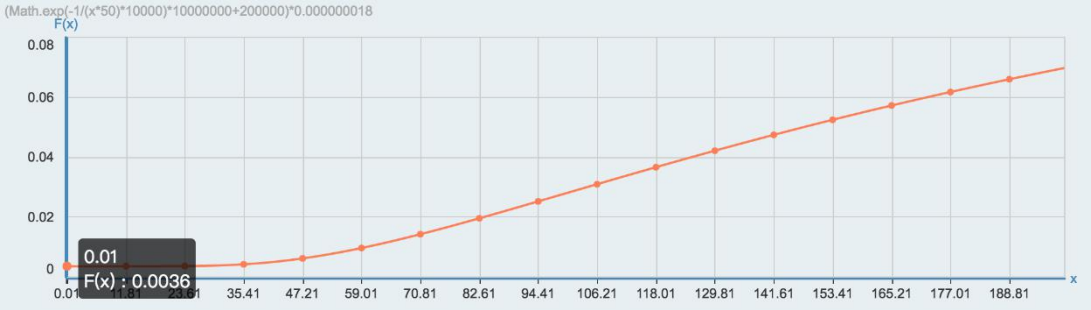
For example, a general transfer of Gas is 21000 and GasPrice is 18Gwei

18Gwei = 0.000,000, 018 ether

A normal transfer requires power = 21000 * 0.000000018 = 0.000378 ether

Power upper limit (ie PowerMax) for one account is calculated as:

PowerMax = (Math.exp(-1/(x*50)*10000)*10000000+200000)*0.000000018

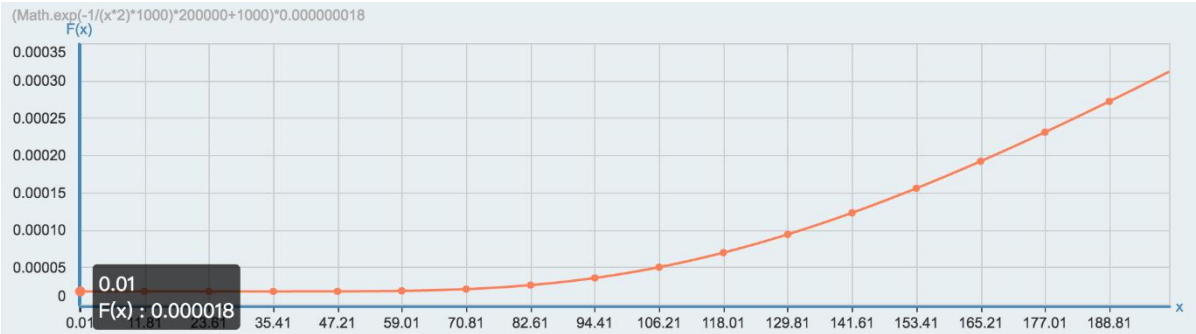


For example, an account with a balance of 0.01etz, PowerMax is 0.0036 ether, assuming GasPrice is set to 18 Gwei (i.e. 0.000000018 ether), the single transaction of this 0.01 ETZ balance can be set to Max = 0.0036 / 0.000000018 = 200000, so the GasPrice is 18 Gwei. In this case, this account cannot send transactions with more than 200,000 gas.

Assuming that GasPrice is set to 36Gwei (ie 0.000000036 ether), the single transaction for this 0.01 ETZ balance can be set to Gas = 0.0036 / 0.000000036 = 100000. We may assume to generalize it, so the GasPrice is 36 Gwei, this account cannot send transactions with more than 100,000 gas.

Power recovery speed of an account (ie PowerSpeed) is calculated as:

PowerSpeed = (Math.exp(-1/(x*2)*1000)*200000+1000)*0.000000018



For example, an account with 0 balances receives 0.01 ETZ at a block height of 100:

- Power of this account at block height 101 = (101 - 100) * 0.000018 = 0.000018;
- Power of this account at block height 102 = (102 - 100) * 0.000018 = 0.000036;

- Power of this account at block height 201 = (201 - 100) * 0.000018 = 0.0018;
- Power of this account at block height 301 = (301 - 100) * 0.000018 = 0.0036;
- Power of this account at block height 401 = (401 - 100) * 0.000018 = 0.0036 (will not continue to grow);

After the block height of 301, the upper limit has been reached. If a user needs to upgrade Power, this user needs to increase its account balance.

Balance-Power Comparison Table (Reference)

Power - Balance under ETZ can be a relation between an account balance with its (gas) Power. Below table can be used as a basic reference:

Balance(etz)	MaxGas	GasPrice	MaxPower	Speed	Max TXs per block	Avg TXs per block
0.01	3,600,000	0.000000001	0.003600000	0.000018000	171	0.86
1.00	3,600,000	0.000000001	0.003600000	0.000018000	171	0.86
10.00	3,600,000	0.000000001	0.003600000	0.000018000	171	0.86
20.00	3,608,172	0.000000001	0.003608172	0.000018000	172	0.86
30.00	3,829,074	0.000000001	0.003829074	0.000018000	182	0.91
40.00	4,812,830	0.000000001	0.004812830	0.000018013	229	1.15
50.00	6,896,815	0.000000001	0.006896815	0.000018163	328	1.64
60.00	10,021,319	0.000000001	0.010021319	0.000018865	477	2.39
70.00	13,937,871	0.000000001	0.013937871	0.000020846	664	3.32
80.00	18,375,300	0.000000001	0.018375300	0.000024950	875	4.38
90.00	23,106,244	0.000000001	0.023106244	0.000031917	1100	5.50
100.00	27,960,351	0.000000001	0.027960351	0.000042257	1331	6.66
150.00	51,047,485	0.000000001	0.051047485	0.000146426	2431	12.15
200.00	69,818,299	0.000000001	0.069818299	0.000313506	3325	16.62
250.00	84,479,214	0.000000001	0.084479214	0.000505207	4023	20.11
300.00	96,015,081	0.000000001	0.096015081	0.000697952	4572	22.86
350.00	105,249,262	0.000000001	0.105249262	0.000880744	5012	25.06
400.00	112,775,519	0.000000001	0.112775519	0.001049417	5370	26.85
450.00	119,012,470	0.000000001	0.119012470	0.001203095	5667	28.34
500.00	124,257,608	0.000000001	0.124257608	0.001342366	5917	29.59
600.00	132,575,636	0.000000001	0.132575636	0.001582554	6313	31.57
700.00	138,865,913	0.000000001	0.138865913	0.001780350	6613	33.06
800.00	143,784,141	0.000000001	0.143784141	0.001944941	6847	34.23
900.00	147,732,733	0.000000001	0.147732733	0.002083512	7035	35.17
1000.00	150,971,536	0.000000001	0.150971536	0.002201510	7189	35.95
2000.00	166,470,735	0.000000001	0.166470735	0.002821683	7927	39.64
3000.00	171,991,257	0.000000001	0.171991257	0.003065334	8190	40.95

For reference only, in the actual operation, it might changes according to service requirements.

From the table, you could find that an account with a 0.01ETZ balance could consume a maximum of 3.6 million Gas for a single transaction (assuming GasPrice was set to 1Gwei).

3. MASTER NODE AND MPoS CONCENSUS

The latest EtherZero is working on the combination of Masternode and PoS. We considered and call ETZ as a MPoS blockchain platform.

3.1 MASTERNODE

A masternode is similar with a node but it has a very important job and additional order on ETZ network consensus.

3.1.1 WHAT IS MASTERNODE?

The masternode, a concept derived from Dash's full-node server, exist at the necessary service facility to ensure that the blockchain provides certain services and basic performances. In the Dash network, the masternode operates based on the PoS (Proof of Stake) mechanism and forms a conceptual double-layer network together with the miner node responsible for completing the POW (workload proof). The requirement to become the Dash coin master is to hold 1000 DASH coins and set up the server as required.

Unlike Dash coins, the EtherZero's masternode is more similar to the super node of EOS[5]. Under the MPoS consensus mechanism, the masternode group replaces the miner role in the PoW mechanism to jointly handle transaction verification, and broadcast work.

The EtherZero's masternode server requirements is not necessary like EOS which requires to reach the data center level, general cloud service can meet the requirements, and the lower node server requirements allow the network to be more decentralized so ETZ is more widely open to public.

3.1.2 MASTERNODE RESPONSIBILITES

The responsibilities of the masternode including:

- Transaction Verification: Verify the signature of the transaction, account balance, Nonce value, etc., execute the transaction and smart contract, and using legitimate transaction to perform block generation;
- Community autonomy: Community has voting rights on the proposals, so the proposal will reflect the community's discussion trends and focus, and will involve all aspects of EtherZero's development, including but not limited to the direction of technical iterations, operation plan adjustments, member dispute resolutions, changes in economic parameters, etc.

[5] Block Producers (BPs) - EOS whitepaper

3.1.3 RIGHTS AND INTERESTS OF MASTERNODE

The construction and maintenance of masternode require the investment of financial resources, time, energy and technology to provide more and better services to users and developers within the whole chain.

75% of the ETZ block generated will be awarded to the masternode. Due to the consensus algorithm, the blocks generated by the poor performance of the masternode are easily discarded, so the blocks generated by the masternode with better performance and network conditions are recognized with higher probability, and more rewards can be obtained.

3.1.4 OPERATING MASTERNODE

There are requirements for becoming the masternode of EtherZero

- Holds 20,000 ETZ;
- Deploy a cloud server. The server should have an independent IP address;
- At least 16 GB of RAM; and
- 1 TB of hard disk space should be available.

For details, please refer to the community's for further details, please refer to **ETZ formal announcement** [6] [7] [8] [9].

3.2 MPoS CONCENSUS MECHANISM

EtherZero 2.0 version is having an MPoS Concensus to govern the block generation and verification.

3.2.1 BLOCK GENERATION AND VERIFICATION

To explain the implementation logic of the MPoS algorithm, we need to first introduce the two traditional methods of block generation on Ethereum.

[6] Offical Announcement On Masternode's Lastest Code Update - https://medium.com/@etherzero/offical-announcement-on-masternodes-lastest-code-update-3b3c244b6780

[7] Step By Step Tutorial | How To Update EtherZero Masternode Code - https://medium.com/@etherzero/step-by-step-tutorial-how-to-update-etherzero-masternode-code-e1c090b1d9d6

[8] How to synchronize the Masternode time - https://medium.com/@etherzero/how-to-synchronize-the-masternode-time-13d36cb40153

[9] Masternode github repository - https://github.com/etherzero-org/go-etherzero/releases/tag/v2.0.3

The first is to connect all the transactions and blocks one after the other from the creation block. This approach has proven to consumes a lot of resources in a complex network such as Ethereum.

The second is that only authorized-machines have the right to generates block, and the nodes will be authorized or de-authorized by voting. These additional voting mechanisms are recorded in the extra data field of the block. In this way, the difficulty of block generation and maintenance cost of the network are reduced.

The nodes only need to download the block headers and verify their validity. After that, you can download an arbitrary recent state from the network and check the nearest header. This consensus mechanism is currently running in Ethereum's test network called Clique.

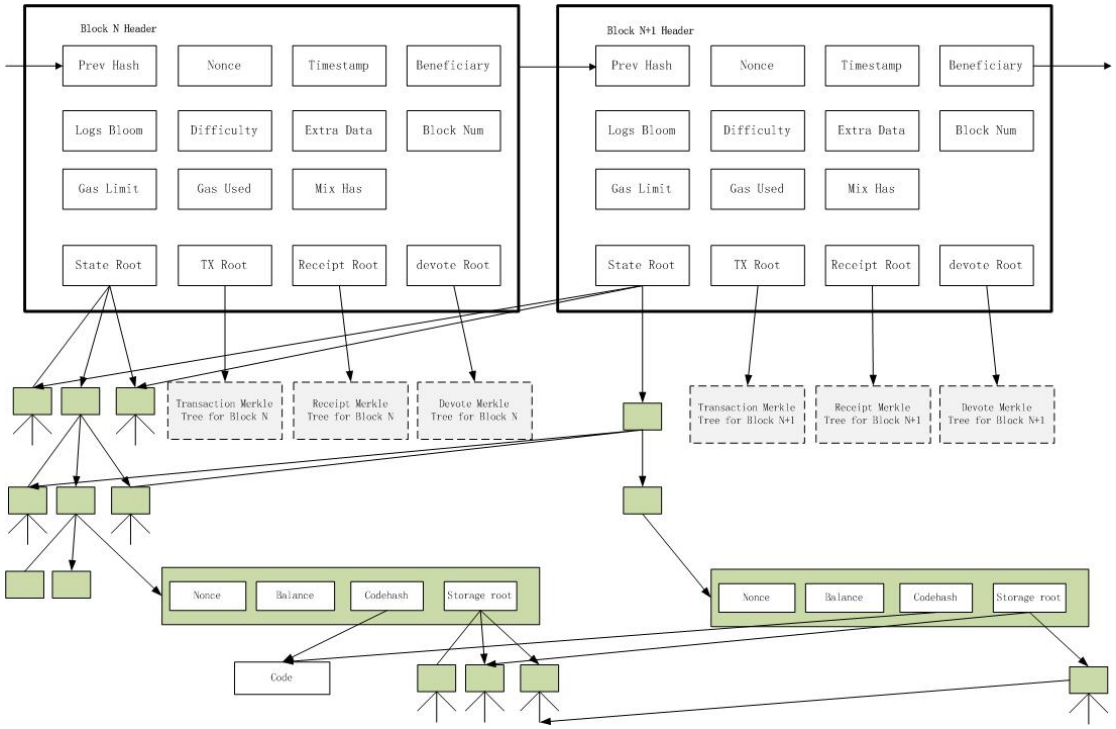
EtherZero's MPoS consensus algorithm is based on the second idea that blocks can only be done by trusted signers, and each block seen by each node can be matched against a list of trusted witnesses. The challenge here is how to maintain a list of authorized witnesses that can be rotated instantly.

We use a system intelligence contract to guarantee that the protocol for maintaining the authorized witness list for each round is included in the block, while in the zone. In the ExtraData section of the block header, we put the signature of the node into it.

This will allow any node that gets a block to authenticate against the list of authorized witnesses. At the same time it also invalidates the field of the miner address in the block header. This also increases the security of the primary node account from another perspective.

3.2.2 BLOCK COMPOSITION

The following figure illustrates the EtherZero block data structure:



3.2.3 AUTHORIZATION POLICY

In order to ensure that the list of authorized witnesses is dynamically and randomly changed, we use the hash value of the block to calculate with the masternode ID and sort according to the calculation result, thus ensuring the unpredictable and random witness list.

It also ensures that the results calculated by all nodes are the same and the consensus is reached.

As long as the witnesses meet the above specifications, they can authorize and assign the blocks they deem appropriate, reducing network traffic and forks by adopting the following strategies:

- Calculate the best signature time for the next block (parent + BLOCK_PERIOD);
- If it is the turn, wait for the exact time to arrive, sign and broadcast immediately;
- If not, delay the time signature of Random(SIGNER_COUNT * 500ms). This strategy will ensure that the current turn of witnesses has a slight advantage over signatures and dissemination.

3.3 INSTANT CONFIRMATION

During each one-hour voting period, 21 masternodes selected by the random authorization algorithm are out of the block, and the block time is 1 s. Once a transaction has been confirmed by 15 different

identities, that is, after verification by 15 different entrants, the transaction is considered to be completely final and unchangeable.

However, in the actual processing, the trade side can flexibly customize number of confirmed blocks required. For transactions with low importance and high real-time requirements, the minimum number of block confirmations can be set to 3 (three). In fact, if a transaction has been confirmed by 3 blocks, its confirmation has reached more than 99%.

3.4 HIGH SCALABILITY

It is based on the 1s outbound time, a safe and efficient consistency algorithm, in the current normal operation of the EtherZero network, the actual TPS can reach 1400.

3.5 HOW TO PREVENT ATTACK

The EtherZero 2.0 version has a high security level protection. The mechanism of MPoS itself is a combination of speed, scalability and security protocol.

3.5.1 51% ATTACKS

The existence of the threshold of the masternode makes it extremely expensive to initiate an attack based on building a large number of nodes. In EtherZero, when the total number of masternodes are 3000, in order to obtain an attack success rate of 1.72%, the hacker needs to control or create 2000 masternodes, this means that the attacker should purchase 40 million ETZs, which is close to 1/5 of the total ETZ circulated.

It is definitely a real big effort to attack the network with a small probability of paying huge economic costs. Combined with the locked ETZ, the overall possibility of attack is reduced, and this kind of attack becomes even more unrealistic.

Number of attack nodes / total number of nodes:

Number of attack nodes / total number of nodes	Success rate p	The amount of Dash required
10/1010	3.44e-24	10,000
100/1100	2.52e-11	100,000
1000/2000	9.55e-03	1,000,000
2000/3000	1.72e-02	2,000,000

$$p=\prod_{i=1}^{n}\left((r-(i-1))/(t-(i-1))\right)$$

Where: n is the length of the masternode chain; t is the number of active masternodes in the current network; r is the number of bad nodes controlled by the attacker,and its value $\geq n$

3.5.2 DOUBLE SPENDING PROBLEM

Bitcoin prevents double-spending problems through PoW and block confirmation. Due to its design limitations, transaction confirmation, network needs to wait for a longer time.

EtherZero adopts the same scheme as ETH to reject double-spending transaction - Nonce value, this kind of scheme description is one account's transaction in the network are executed based on the sequence of transaction, and this scheme is also to cancel Pending transactions which are not processed for a long time and provides the possibility to carry out a transaction by setting a higher Gas Price to replace Pending transaction with the same Nonce value.

3.5.3 SYBIL ATTACK

Refers to an attack that benefits from creating multiple accounts on the network. Single-account transaction ability attenuation feature constructed by the Power mechanism will result in a more effective sybil attack only by holding a large number of ETZs, and the trading pool which run the transaction order based on Gas Price will further reduce the impact of the attack.

3.5.4 DDoS ATTACK

A DDoS attack refers to a large number of spam requests to host server in a short period of time, which may cause some of the master nodes goes offline and service disruption. Because of the Gas and Power mechanisms, DDoS-type attacks have small influence on EtherZero network.

3.5.5 FINNEY ATTACK

The Finney attack is named after a Bitcoin user, Hal Finney, it is an attack that exploits unconfirmed transactions in Bitcoin to fraudulently accept bitcoin payments, a variation of a double-spending attack. The precondition for this attack is that the merchant trusts the

unconfirmed transaction and immediately ships the shipment after receiving the unconfirmed transaction and cannot be revoked.

This is actually using the time difference of the high-latency transaction confirmation service such as BTC. In the EtherZero, the near real-time transaction greatly reduces the possibility of this attack.

4. COMMUNITY AUTONOMY AND EVOLUTION

Thanks to the support of smart contracts, EtherZero community autonomy can be solved entirely through client Dapp and online wallet.

The approach to governance is through,

- Increased focus on masternode proof of stake (MPoS) by EtherZero community;
- Responsible EtherZero leadership team making decisions and risk appetite.

4.1 PROPOSAL INITIATION

- Anyone can initiate a proposal;
- 1.2 million blocks has one vote, vote counting period is around two weeks;
- If the proposal failed to meet the requirements within the period, it need to be resubmitted;
- The budget requested by each proposal cannot exceed current available budget.

4.2 MASTERNODE VOTING

Any masternode has one vote for each proposal in the current period, which can be used to approve, against, or abstain.

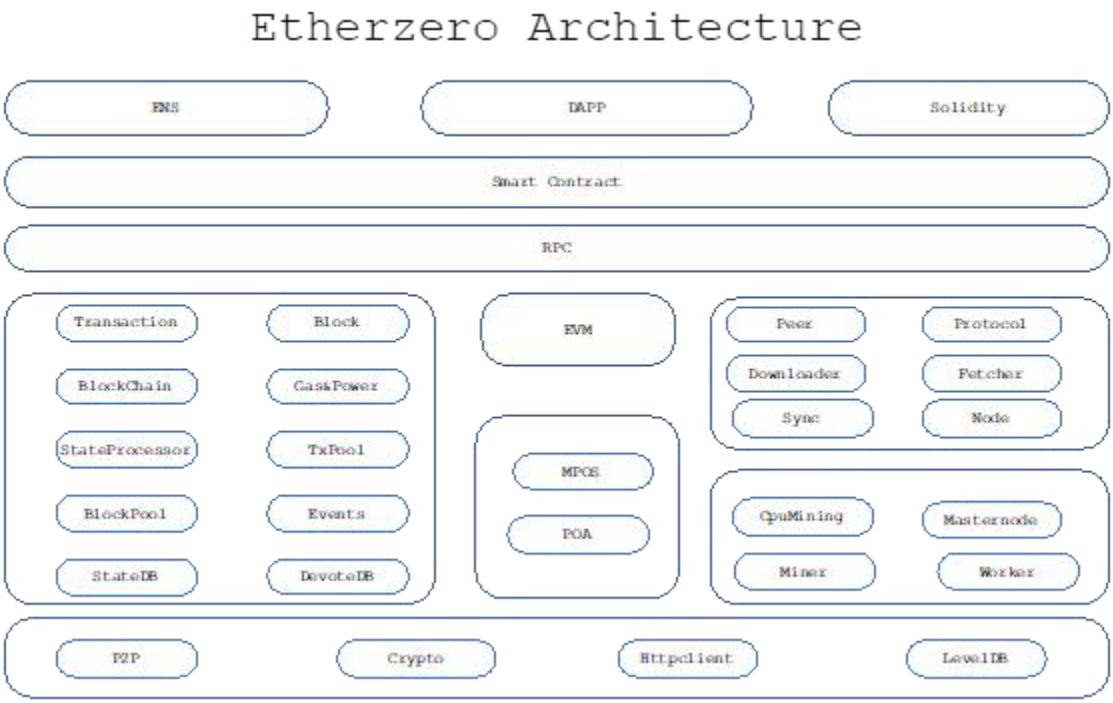
4.3 VOTE COUNTING AND BUDGET APPROVAL

The eligible proposal has criterias as below:

- Total number of votes which approve proposal – Total number of votes which against proposal > 10%;
- For all proposals that meet Condition 1, will be sorted based on the difference in the votes and the current available budget will be given based on the order. After the release is completed, if the remaining budget does not meet the budget requests of the next proposal that meets the above conditions, then budget will not be awarded and the remaining budget will be added to the next period;
- The vote counting is performed in the last block of each cycle. Community Governance Contracts will give awards to the eligible proposals.

5. TECHNOLOGY AND ECONOMIC PARAMETER

5.1 TECHNICAL STRUCTURES



5.2 CONCENSUS PARAMETER

- The EtherZero 2.0;
- Consensus mechanism: MPoS;
- Signature algorithm: Secp256k1;
- Hash algorithm: Sha256;
- Voting period: around 1 hour;
- Number of blocknodes: 21, each voting period is randomly rotated from all the masternodes according to the algorithm;
- Required different block masternode/number for final confirmation: 15.

5.3 BLOCK PARAMETER

- Block generation time: 1s;
- Block generation reward: 0.45 ETZ;
- Reward allocation: 75% is distributed equally to the online master node; 25% for the community budget.

5.4 MASTERNODE PARAMETER

- Threshold 20,000 ETZs;
- Basic requirements: RAM is larger than 16G, hard disk is not less than 1TB, 8-cores CPU.

6. ECONOMY SYSTEM

6.1 CURRENCY USAGE

The use of ETZ coins throughout the ecology is categorized by the roles involved:

1. Masternode
   a) needs to hold a certain amount of ETZ
   b) as block reward will be rewarded to the masternode

2. Developer

   needs to hold a certain amount of ETZ in order to have the basic power needed to deploy the contract

3. User
   a) You need to hold at least 0.01 ETZ in order to have the basic Power to initiate the transaction. The more coins you hold, the more transactions you can initiate per unit of time, the higher transaction complexity that can be initiated;

4. Community;
   a) As budget for the eligible proposals approved by the community.

An economy system based on the above functions can effectively motivates each role to work for a common goal within the EtherZero ecosystem.

6.2 MONEY SUPPLY

EtherZero or abbreviated as ETZ, initially issued with total of 194 million, of which 97 million are distributed as 1-2 equals to the Ethereum holder after the fork. The remaining 97 million ETZ is distributed for private placement of early investors, EtherZero Foundation, EtherZero Post Development and Eco Development.

Block reward will add approximately 12 million ETZ per year, with 75% of each block output for the masternode and 25% for the community autonomy budget.

6.3 CURRENCY LOCK

EtherZero coins are locked under a smart contract when joining the Masternode and Power mechanism.

6.3.1 MASTERNODE LOCK

Dash currently has 4,777 masternodes (December 2017), and each masternode needs to lock 1000 Dash, accounting for 61% of the total amount of Dash, 7,783,295 coins (December 2017).

In EtherZero each masternode needs to lock 20,000 EtherZero coins, assuming after 1-year operations, EtherZero operating 4000 main-nodes or masternode, therefore it needs to lock 80 million ETZ, accounting about 41% of the total ETZ.

6.3.2 POWER LOCK

Based on the Power mechanism, all operations on network computing, storage, and bandwidth resources, such as transactions or deployment contracts, will consumes Power. The Power max and Power speed of an account depend on the number of ETZs held by the account. Therefore, the Power mechanism will cause a large number of ETZs to be locked into the account.

6.4 MONETARY POLICY

The coin-locking behavior of various roles such as masternodes, common users, and developers causes the market supply to maintain a certain amount of deflation for a long time. As the business grows, the value of these locked coins will be adjusted through the community's voting system.

It can be seen from the above that there will be most of the EtherZero ETZ stored in the masternode and the smart contract. This endogenous economic system, together with the steady flow of new accounts, the payment demand for the ETZ and the trading platform, New investors will demand ETZ and it will continue to push up the price of ETZ.

7. TECHNICAL CHARACTERISTICS

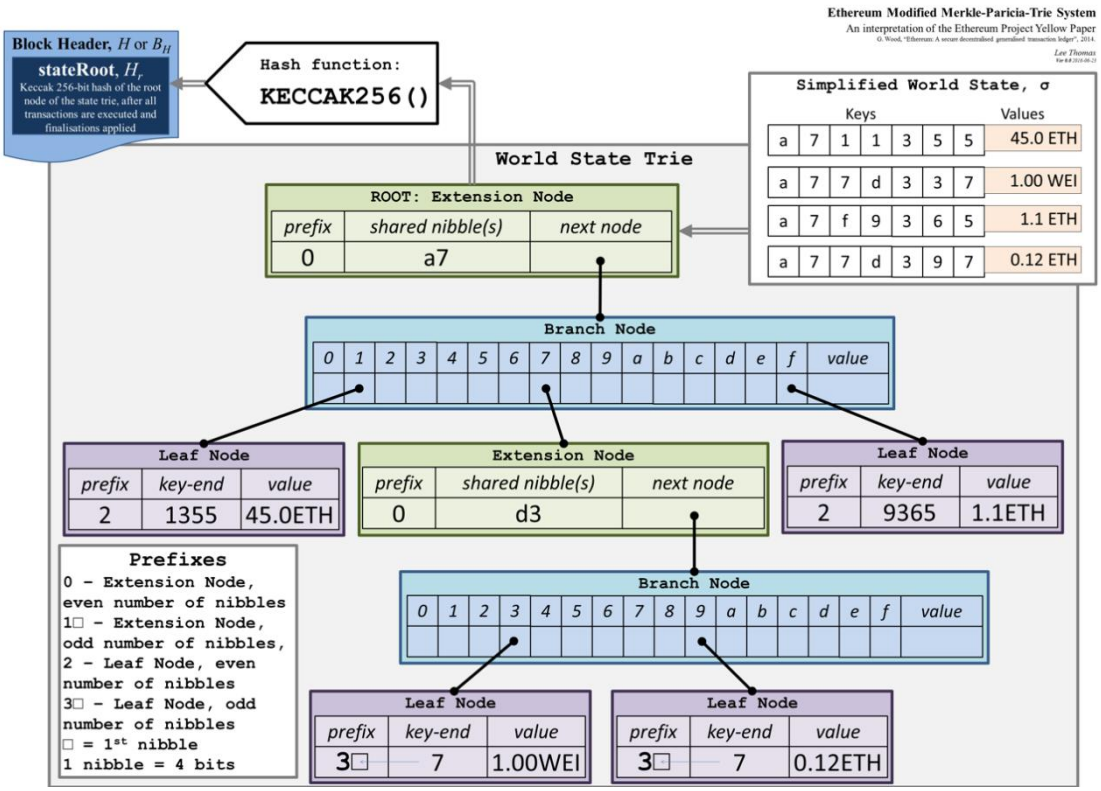
7.1 TECHNICAL CONSIDERATIONS

After considering Ethereum's performance, EtherZero has put in place a number of mitigating factors: Our current block generation time is 1s, and EtherZero has further considered the data reading speed of Ethereum EVM in executing smart contracts and the core issues affecting Ethereum performance.

In the bitcoin system, the execution time of Bitcoin scripts is never considered in the transaction delay time problem of Bitcoin networks, mainly because bitcoin scripts are non-Turing complete and very short, and the implemented-functions naturally are very simple.

Ethereum is an account model that is itself a state machine and supports Turing's complete on smart contract. Compared to the bitcoin script, the Ethereum uses WorldState to use MPT (Merkle Patricia tree) to record the entire Ethereum state change.

Ethereum's EVM spends a large part of the time spent executing smart contracts on reading network-state. The following figure depicts the storage of the MTP state tree root hash:



Note: Image comes from Ethereum Stack Exchange.

Since this unique data structure will increase with the amount of transactions recorded, the number of interactions with the underlying database per read for a specific value will increase by O(n). These accesses are not sequential storage but discrete random storage. The underlying leveldb is very low in performance when faced with such a large number of data reading.

At present, the miners in Ethereum are paying more attention to HashRate in order to ensure the block generation rate. However, this block is completed by the GPU, therefore, it is not very concerned about

the overall performance of the data reading when the smart contract is executed. Solving this problem and further improving the processing speed and stability of the network will be the next goals of our team.

7.2 WORK ARRANGEMENT

The technical characteristics of the platform iterative rollout will correspond to the ecosystem's progressive development plan, guiding developers and users to pay attention to the killer application supported by the corresponding features based on different characteristics at different periods. EtherZero will look at the organic growth of ecosystem from a development perspective.

8. APPLICATION SCENARIOS AND MARKET EXPECTATIONS

EtherZero Team believe that the development of ETZ will make the blockchain technology to its new height and it can bring blockchain service to next level.

You can imagine that a small service or activities are required in the multimedia interaction and it will not be feasible under current fee blockchain or cryptocurrency scheme. ETZ will release the true power of blockchain.

8.1 GENERAL APPLICATION

The core task of the blockchain is that trust is irrelevant, which is, no matter who the counterparty is, the party don't need to generate trust but can directly do trading. This can be carried out through smart contracts. Take a match result for a gambling contract as an example. The simplified code is as follows:

```
Match result = NBA official website API.get ("final")
If (Knight wins)
  Pay 40 to A
Else
  Pay 40 to B
```

In this regard, in reality, any trades who need two or more parties to participate, need a middleman to prevent distrust. These kind of transaction can utilize smart contracts on blockchain to replace the middleman's duties.

In fact, the smart contract based on Ethereum is also universal, but its cost-consuming features make the complex smart contracts written by developers unable to support large users in terms of cost, such as for gamers.

But after EtherZero removed its transaction fee system, users who use smart contract services will not pay any cost, ensuring the economic viability and sustainability of large-scale decentralized applications, and making Dapps naturally have the ability to differentiate services based on account balances.

8.2 INDUSTRIAL APPLICATION USE CASES

EtherZero is a base layer application development platform. While it is not limited to the enterprise level collaboration, it is necessary to have well-considerations. This kind of considerations is an application that we will start to work with in the future.

8.2.1 GAME PROP CONTENT COLLABORATION AND TRADING PLATFORM

A cat application has stirred up the entire Ethereum, and it has also made people realize the great potential of the blockchain in the game segment, the importance of its uniqueness in the non-fungible digital asset transaction market.

We will design a content-based decentralized prop outsourcing and trading platform that connects designers and scriptwriters, numerical system designers, game makers, players, etc., for each role, for example:

- Game manufacturers: release demand, lock ETZ coins to smart contracts as pre-payments;
- Designers and screenwriters: pick up the tasks, design the props according to the game concept of the game manufacturer; accept the contract payment after confirmation;
- System designers: design explosion rate, prop effect, explosion requirement, variation requirement, variation rule, etc.; accept the payment of smart contract after confirmation.
- Player: Vote for prop design; trade unique props;

Through this ecosystem, community can express and spread new ideas.

8.2.2 INDUSTRY TOKEN PAYMENT SOLUTION

Study and research thoroughly with various experts from various industries to discuss the necessity and feasibility of EtherZero economic system establishment in the industries. It also explores the combination of big data technology and distributed accounting, anonymous accounting technology, and provides sufficient input for the industry's artificial intelligence applications based on a large amount of trusted data.

8.2.3 CENTRALIZED ORGANIZATION MAPPING

Society needs various forms of organization. The inclusiveness and diversity of society itself is a manifestation of the degree of social freedom. We plan to implement a virtual mapping of real-world organizations in EtherZero. Compared to DAO organizations, we call this mapping as MRO (Map of Real world Organization). This implementation can cover anonymous and real names and can help existing enterprises to quickly Application of blockchain technology to achieve enterprise management and business relationship management. Imagine:

1) Each organization can map its own organization to the app

2) Organization management
   a. Recruit members and sign a smart personnel agreement
   b. The organization can issue remuneration through the platform to carry out various equity structures
   c. Purchase of various big data, artificial intelligence services based on standard trusted chain data developed by developers and lawyers.
   d. Issue outsourcing tasks and sign smart outsourcing agreements
   e. Initiate a registered and secret ballot

3) Between organizations
   a. Can sign a smart contract with a commercial counterparty without third party guarantee
   b. Can sign smart agreements such as equity mutual ownership with partners
   c. Issue corporate debt, ICO and various types of financing

4) More virtual, protocolizable scenarios.

9. TEAM

As a global public blockchain network project, EtherZero is developed by the core development team from China and two senior DAPP development teams from India and Eastern Europe to help on the research and

development, and at the same time, a numerous domestics and overseas marketing teams work on the promotion and operation of DAPP base layer development platform.

9.1 ETHERZERO CORE TEAM

Befree– Team Leader

A serial entrepreneur, from universities drop-out to entrepreneur, has engaged in online marketing, shareware, mobile games to cryptocurrency, where he in charge for the development and operation of several altcoins and DAPP. Responsible for the design of EtherZero concept, the direction of development, and strive to promote EtherZero as DAPP base layer development platform, and continue to improve and develop in 5-10 years or longer, give contribution to the next generation of blockchain network society.

Online Reference: Linkedin.

Rolong - Technical Director

A senior full-stack development engineer with more than 10 years of development experience, proficient in server-side development such as C++, GO, JAVA, Erlang, etc., and web3, h5 and other front-end development, senior intelligent contract developers, have in-depth research on the underlying network of Ethereum, and even in China he is considered as top DDoS defense expert, his published technical solutions are are treated as technical standards by other developers.

Roger Luo - Development Director

The senior Ethereum base layer development engineer is a domestic technical bureau with a lot of technical research on the base layer of Ethereum. Ten years of experience in financial technology development, blockchain enthusiasts, active members of the open source community, focusing on the EtherZero core development

Frank - Product Manager

Two years of experiences as financial industry consultant, 3 years' experience working as financial industry product manager, now focusing on the application scenarios of cryptocurrency and blockchain technology, and possible technical implementation paths.

Mia - Senior Overseas Marketing Specialist

Has many years of experience in overseas promotion and has achieved excellent results, responsible for the promotion of EtherZero network

9.2 ETHERZERO SUPPORTING TEAM

Advisor 928 (Sydney – Australia), Blockchain and Community Enthusiast

General interests in cryptocurrency, blockchain distributed ledger technology and community led technical or end user training and development on safety and use of cryptocurrency.

Asonganyi Derick (Cameroon- Cameroon), Community Manager

Senior Site Manager at Global E-commerce network

I am an enthusiast who started the venture of making money online some 4 years back since then, I have been involved in multiply online money-making activities. Got involved in to the Crypto world in 2014 and has been involved in almost all aspects of the community ranging from trading, teaching and project contributions. still very much in love with Crypto technologies I am also a social medial 'influencer' involved in activities like building and management of social medial accounts.. Writing is a call. I do technical (white papers for project mostly crypto related) and article writings.

Specialities: Key Competencies: Blockchain distributed ledger technology, Technical Project Manager, application and hardware appliance upgrades, supply chain integration services, CMS and legal services.

Online Reference: Linkedin.

Bryan Vukich (Greater Milwaukee Area - USA), Community Manager & Operations Consultant

Senior Network Engineer

Senior Network Engineer with over 20 years total IT experience. Experienced in server and network operations, network design and security, and risk mitigation. Over 6 years cryptocurrency experience as a user, miner, trader, and node operator.

Online Reference: Linkedin.

Email: bryan@etherzero.us

Evgeny Egorov (Moscow - Rusia), Tech & Operations Consultant

Entrepreneur, Chief Executive, crypto enthusiast

Over 20 years IT experience. First 10 years – implementation of ERP systems, a lot of projects in many industries, work for three IT giants – Microsoft, Oracle and IBM. Last 10 years – own telecommunication business, creation fully automated complex system of traffic management, online Business Intelligence, tests and routing monitoring. 3 years cryptocurrency experience as a miner, and trader. From beginning of 2018 – active ETZ fan with dream of integration telecom business with EtherZero platform.

Email: evgeny@etherzero.ru

Pfistl Falterhauser (Germany), Blockchain and Community Enthusiast

Adviser Promotion and Community, Translator and Editor/Author of German Texts. Crypto Enthusiast since 2016.

Experience with Miners and Masternodes.

More than 11 Years of Experience in the field of Medical Care and preventive measurement for critically ill people with Oxygen Devices and Respiratory protective Devices, Monitoring, Homecare.

Special Training for Palliative care, Child care, Geriatric care and General care.

Rikrik Gantina (Jakarta – Indonesia), Marketing Supporter and Blockchain Enthusiast

Technical Lead in Oil and Gas Industry

A Blockchain Enthusiast since 2013, with more than 15 (fifteen) years experiences in Oil Gas industry, particularly in Large Scale Offshore/Onshore Subsea Tie Back Projects, Subsea Field Developments, LNG Based Development, FSRU (Floating Storage and Regasification Unit), Subsea Fiber Optic Project.

Online Reference: Linkedin.

Email: rik@etherzero.id

Tsutomu Tagashira (Shinjuku - Tokyo, Japan) - Community Enthusiast

Artist, Musician, and Composer (Music Composer)

Attenting and/or composing seeral International Film and/or Music Festival around the word.

Online Reference: FB.

10. Roadmap and Milestones

Period/Month	**NEXT STAGES**
2019 Q1	• In the first quarter of 2019, the star Dapp app contest and launched a long-term developer reward program. • Study the combination of DAG consensus mechanisms and smart contracts, and how to integrate block and consistency. • Study techniques such as Plasma Layered Network to improve TPS. • Study on how to implement fragmentation techniques in a masternode network. • Study on how the architecture and business sidechains are structured in an Ethernet network and the feasibility.
	ACHIEVEMENT
2018 Q1	• In January 2018, the EtherZero test network was released to the public, implementing zero transaction costs and anti-DDOS attacks.
..... Feb	• In February 2018, the EtherZero private placement was completed, the online wallet was launched, the main online line carried out 0 transaction costs and anti-DDOS attacks, and the first forked zero Ethernet block was dug out.
..... Mar	• In March 2018, the mobile version of the wallet was released, and the Dapp application market was promoted to further develop the user UX environment.
..... Aug	• In the first quarter of 2018, the master node (Master Node) was successfully tested on Testnet
2018 Q2	• In the second quarter of 2018, the master node (Master Node) Go Live on the Mainnet to achieve real-time transactions and higher transaction concurrency (greater than 1000 TPS).
2018 Q4	• In the fourth quarter of 2018, the master node Master Edition optimized online, supporting thousands of TPS.

11. CONCLUSION

EtherZero combines the best of Ethereum builds with a safe and reliable free from transaction cost, making the large and complex smart contracts economically viable, stable and continuous, the high scalability and real-time transaction feedback realized by the master node network. A large number of users will have an excellent interactive experiences, which will change the impression that the blockchain transaction confirmation waiting time is too long.

Blockchain industry is still in the early era and it is struggling to face the technology challenges, only by build it on the well-established technical approaches, step by step understanding deeply about the industry, the blockchain technology can reduce the overall risks-faced, and complete long-term goal of becoming the mainstream blockchain application platform.

The limitations of current technology will limit the popularity of blockchains in daily life, and price-speculations will continue for a long period of time.

EtherZero will not forget the original objective, aiming at improving the blockchain technology, exploring the application in various industries as its own responsibility, using decentralized technology and ideas to improve social operation efficiency, reducing the cost of social operations, and contributing a little to achieve a fairer society.

Thanks for your support!