Ethercoin

White Paper

Contents

Abstract

This document describes Ethercoin or ETE as the evolving platform for the implementation of a general smart contract development, high transaction processing capacity, near real- time transactions.

While Bitcoin (Peer-to-Peer Electronic Cash) solved the double spend problem and provided work with timestamps on a public ledger, it has not to date extended the functionality of a blockchain beyond a transparent and public payment system. Satoshi Nakamoto's original reference client had a decentralized marketplace service which was later taken out due to a lack of resources. We continued with Nakamoto's vision based on Ethereum.

By using ProgPoW as a consensus participant, it can significantly lower energy consumption and entry barrier, making mining of crypto currency safer, more decentralized and for everyone. Ethercoin generates its unique value through mathematics and code. This White Paper will explain and elaborate on the monetary and technical attributes of ETE.

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

Ethercoin extends the Gas mechanism of Ethereum, and extends the concept of Cash 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. An Ethercoin consensus algorithm based on ProgPoW is designed and implemented.

This consensus algorithm enables standard transaction exchanges between accounts as well as empowering the community with autonomy to run miners. A pre-requisite to be a miner participant is to hold an agreed amount of Ethercoin coins and running it on a performance compliant hosted server. Currently, based on network parameters such as ProgPoW consensus and properly set out block time, Ethercoin can achieve a high degree of decentralization with a high number of miners and with transaction processing capabilities of above 10,000 TPS.

ETHERCOININTRODUCTION

Ethercoin (ETE) is Smart Electronic Cash, has strict Deflationary Monetary Policy. ETE 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. Protected by native internet hash power, ETE Team is aware of the needs to always maintain the platform to thrive the challenge for the needs of high-quality requirement including security.

ETE is always evolving; ETE always improves to cope the blockchain platform and its application needs.

PROJECT BACKGROUND

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

Ethereum can't resist ASIC

When numerous resources are being used in the mining procedure and costs are gradually increasing, crypto currency enthusiasts have started looking for alternatives to lower power consumption in two different ways: either using new consensus to lower energy cost or using more general apparatus to lower the cost of mass production. The golden age of ASIC mining device and anti-ASIC algorithm implementation had come. The original intention of Ethereum was to resist ASIC, using a different non-ASIC-friendly consensus to keep the system away from ASIC manufacturers' manipulation while keeping the energy consumption low. However after a period of time, ASIC manufacturers still found ways to design devices that would work with the corresponding algorithm.

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

ETE provides the perfect solution for the issues mentioned above. It brings a method for crypto zealot to make general apparatus while keeping the energy consumption low. Meanwhile, ETE maintains a relatively high difficulty level to ensure the stability of the system by using its consensus Proof of Work (abbr. PoW). The PoW consensus used by ETE is also one of the most decentralized consensus mechanisms in this era. PoW utilizes common computer devices as a more economical consensus method, so that more people can participate in construction of the system stabilizing hash power with their own devices. It was the original intention of Nakamoto to design PoW, a decentralized system and an innovative path to real decentralization for everyone, raising consciousness in every new comer to think about and overturn the existing design. ETE has inherited BTC's spirit, now the new PoW mechanism is responsible for bringing a

better future for crypto currency, and engaging more people in the construction of the economic system.

Ether is the gas instead of cash

The supply of Ether is unlimited

ETHERCOIN KEY FEATURES

Peer to Peer Smart Electronic Cash

Ethercoin is electronic cash. It's used as value store, payment way, and value scale, and the same time, Ethercoin extends the Gas mechanism of Ethereum to the Currency mechanism, and improves the economy system 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. The transaction initiator only needs to hold and the transaction just need to consume the basic currency of the network (ETE).

ETE has different approaches in Ethereum gas mechanism. In Ethereum, the transaction fee is calculated by the value of the Ethers, the mining reward, gas incurred and the gas price, 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:

1. A tool to measure computational resources usage in the network;
2. Converted into transaction fee, as reward for miner and block verification;

3. Converted into transaction fee, as an economical method to resist DoS attacks

In Ethercoin, ETE is used as a computational resources measurement tool and the fee is replaced and expanded by the cash mechanism.

The Peer to Peer Smart Electronic Cash mechanisms established a solid foundation for Ethercoin transaction cost safely.

Deflationary Monetary Policy

Ethercoin sets up strict Deflationary Monetary Policy. ETE has a coin output mechanism similar to that of Bitcoin, i.e. the daily output will be reduced by 50% every two years.

Ethercoin is upgraded from Ethereum. Ethereum community got around 100M air drop. all other coins must be minted by POW mining. Because there is orphan block reward, the total number of ETE will be around 0.5 Billion. Then the mining will only generate the processing fee without issuing new currencies.

As for ETE, there is no interest mechanism during PoW mining, and new currencies are all issued in the new block. It reflects our consideration of ETE internal and external economic systems, and also represents our acceptance of the thought of the Austrian School of Economics.

The production strategy of limited total quantity and deflation contributes to the maintenance and appreciation of asset values of ETE investors, and synchronously avoids inflation and dilution. Similar to ETH, ETE can conduct nine-figure segmentation after the decimal point, without the problem of losing transaction function due to over high value of a single token.

Pow Only

There must be a cost for currency issuance. We choose the energy as the cost of ETE. Pow is better than POS: dynamic and cost. All the hash power must be natively from internet: cpu, gpu, or store ability. Now we choose to

use ProgPOW. ProgPoW is a proof-of-work algorithm designed to close the efficiency gap available to specialized ASICs. It utilizes almost all parts of commodity hardware (GPUs), and comes pre-tuned for the most common hardware utilized in the Ethereum network.

Ever since the first Bitcoin mining ASIC was released, many new Proof of Work algorithms have been created with the intention of being “ASIC-resistant”. The goal of “ASIC-resistance” is to resist the centralization of PoW mining power such that these coins couldn’t be so easily manipulated by a few players.

This document presents an overview of the algorithm and examines what it means to be “ASIC-resistant.” Next, we compare existing PoW designs by analyzing how each algorithm executes in hardware. Finally, we present the detailed implementation by walking through the code.

The design goal of ProgPoW is to have the algorithm’s requirements match what is available on commodity GPUs: If the algorithm were to be implemented on a custom ASIC there should be little opportunity for efficiency gains compared to a commodity GPU.

The main elements of the algorithm are:

1. Changes keccak_f1600 (with 64-bit words) to keccak_f800 (with 32-bit words) to reduce impact on total power
2. Increases mix state.
3. Adds a random sequence of math in the main loop.
4. Adds reads from a small, low-latency cache that supports random addresses.
5. Increases the DRAM read from 128 bytes to 256 bytes.

ADVANTAGE OF ETHERCOIN SOLUTION

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

CLEAR TRANSACTION COST

The most persuasive tool of Ethercoin characteristics is clear transaction cost.

Taking the simplest distributed collaborative to-do list, or to-do application, as an example, its decentralized implementation can be applied to the task decoProgPoWition 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.

ProgPoW CONCENSUS

Ethercoin is having an ProgPoW Concensus to govern the block generation and verification.

Why ProgPow

The PoW algorithm on Ethercoin adopts ProgPoW. The purpose of using ProgPoW is to narrow the efficiency gap between commercial GPU and ASIC miners, to resist the computer monopoly of ASIC miners and to

achieve fairer mining. ProgPoW algorithm is improved by Ethash Algorithm, so the POW consensus algorithm of ETE can switch to ProgPoW smoothly.

ProgPoW is a proof-of-work algorithm designed to close the efficency gap available to specialized ASICs. It utilizes almost all parts of commodity hardware (GPUs), and comes pretuned for the most common hardware utilized in the Ethereum network.

Ever since the first bitcoin mining ASIC was released, many new Proof of Work algorithms have been created with the intention of being “ASIC-resistant”. The goal of “ASIC-resistance” is to resist the centralization of PoW mining power such that these coins couldn’t be so easily manipulated by a few players.

This document presents an overview of the algorithm and examines what it means to be “ASIC-resistant.” Next, we compare existing PoW designs by analyzing how each algorithm executes in hardware. Finally, we present the detailed implementation by walking through the code.

The design goal of ProgPoW is to have the algorithm’s requirements match what is available on commodity GPUs: If the algorithm were to be implemented on a custom ASIC there should be little opportunity for efficiency gains compared to a commodity GPU.

ProgPoW CONCENSUS MECHANISM

Compared with Ethash, its resistance to ASIC is mainly manifested in the following characteristics:

- Change keccal_f1600 (64 words) to keccak_f800 (32 words) to reduce its impact on the total
- calculation power.
- Increase the mixing state
- Adding Random Mathematical Sequences to Main Cycle
- Add low-latency, small-scale cache reads that support random addresses

- Increase DRAM reading from 128 bytes to 256 bytes

In addition, ProgPoW has six definable variables that can be bifurcated to further address threats from ASIC or FPGA. These six variables are as follows:

1. PROGPOW_LANES:
   Number of parallel rows coordinated to compute a hash instance; default value is 32
2. PROGPOW_REGS:
   Register file usage size; default value is 16
3. PROGPOW_CACHE_BYTES:
   Buffer capacity; default value is 16*1024
4. PROGPOW_CNT_MEM:
   The number of frame buffer accesses defined as the external loop of the algorithm; the default value is 64
5. PROGPOW_CNT_CACHE:
   Number of cache accesses per cycle; default value is 8
6. PROGPOW_CNT_MATH:
   Number of mathematical operations per cycle; default value is 8

ANONYMOUS ASSETS AND PRIVACY

The privacy and the transactiontransparency have been emphasized in Ethercoin as well.

Ethercoin provides anonymous assets transaction based on zero-knowledge Succinct Non-interactive Arguments of Knowledge (zkSNARK). It will provide the anonymous assets based on the sidechains. The anonymous asset based on the zkSNARK has greater privacy. Users can issue anonymous tokens based on the Ethercoin sidechain.

Ethercoin sidechain will use Ethercoin cross-chain protocols and connect the other sidechains through the cross-chain protocol. Sidechain can have its own platform token and customized consensus, and can actively customize their own assets and the methods of how their anonymous assets have been allocated.

COMMUNITY AUTONOMY AND EVOLUTION

Because Ethercoin support of smart contracts, Ethercoin community autonomy can be solved entirely through client Dapp and online wallet.

CASH ECONOMY SYSTEM

MONETARY POLICY

Ethercoin Strictly enforces deflationary currency model, halves every two years.

The capped supply amount of ETE causes the market supply to maintain a certain amount of deflation for a long time. As the business grows, the value of these holded ETE will be adjusted through the community's economy system.

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

MONEY SUPPLY

Ethercoin or abbreviated as ETE, initially issued with total of 0.5 billion, of which 20% ETE will be inherited by ETH holders. The ETE miners will be rewarded the 80% of the rest of 80% ETE while the 20% of the rest of 80% ETE will be rewarded to the ETE developers.

CURRENCY USAGE

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

1. Miner
2. Developer
3. User
4. Community;

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

TYPICAL INDUSTRIAL USE CASES

Ethercoin 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.

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

INDUSTRY TOKEN PAYMENT SOLUTION

Study and research thoroughly with various experts from various industries to discuss the necessity and feasibility of Ethercoin 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.

CONCLUSION

The Ethercoin LOGO originates from a diamond double crystal octahedron, which represents solid and untamed, beautiful and eternity.

Ethercoin 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.

Ethercoin will not forget the original objective which is Peer to Peer Smart Electronic Cash, 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.