maketitle

Rethereum Blockchain

Rethereum Team

07/08/2023

Rethereum is a new blockchain project that aims to revive the original vision of Ethereum as a global, decentralized platform for money and new kinds of applications. Rethereum is based on a Ethereum's final release to support Proof-of-Work.

The `Rethereum` project aims to maintain a strong Proof-of-work cryptography blockchain and prove that a stable financial platform can be accomplished in a decentralised event-driven blockchain.

Rethereum isn't just another Ethereum clone, it is a brand new blockchain and brand new ideas to keep Proof-of-work as the backbone of the network for security and decentralisation.

```
Rethereum is based on the Ethereum network and code, by extention
technical details from the Ethereum whitepaper can be considered a part
of Rethereum unless written otherwise. Rethereum remains backward compatible
with Ethereum and such network specific technical details should be
understood from Ethereum's detailed documents. This whitepaper should be
```

Rethereum Team: team@rethereum.org, https://rethereum.org

considered an extention of Ethereums Whitepaper detailing change, plans, ideologies and methodologies.

1 Native Currency

The network runs on a single currency, symbol `RTH`, this is used for transactions, mining, smart contract deployment and execution. The currency has 18 decimal places, which allows for very precise transactions and avoids rounding errors. The currency is mined by solving proof-of-work problems, which secure the network and validate transactions.

The mining reward is initially set to 4 coins per block, but it will gradually decrease over a period of 9 years until it reaches a constant inflation rate of 2.1% per year. This is designed to mimic the natural growth of the economy and to encourage early adoption. The total supply of coins will be 125 million after 9 years, and then it will increase by 2.1% annually. This means the first year of the 2.1% inflation cycle each block will reward 0.58228108671

Additionally, transaction fees are rewarded to the block miner and not burned off the network from EIP-1559. This ensures that miners have an incentive to process transactions and to maintain the network security. The transaction fees are dynamically adjusted based on the network congestion and the demand for block space. This creates a more efficient and fair fee market that benefits both users and miners.

2 Programmable Currency

The main features of our proposed system is a Turing complete programmable currency using smart contracts. Smart contracts are self-executing agreements that are encoded on the blockchain and can perform complex logic and operations. They enable users to create and enforce rules for the transfer and use of the currency, such as conditional payments, escrow services, automated auctions, and decentralized applications.

A Turing complete programmable currency means that the smart contracts can express any computable function and are not limited by predefined templates or functions. This allows for greater flexibility, innovation, and customization of the currency system. Users can design and deploy their own smart contracts to suit their specific needs and preferences, as well as interact with other smart contracts on the network.

The smart contracts also opens up new possibilities for cross-chain interoperability, as smart contracts can communicate and exchange value with other blockchains that support the same programming language and standards.

Another important aspect of our system is the ability to create custom currencies that are backed by the native currency of the network. Users can issue their own tokens that represent a fixed amount of the native currency, and use them for various purposes, such as crowdfunding, loyalty programs, stablecoins, or digital assets.

These tokens are fully compatible with the smart contracts and can benefit from the same features and security of the programmable currency. Users can also exchange their tokens with other users or redeem them for the native currency at any time. This way, users can create and manage their own monetary systems within the network, without relying on third parties or intermediaries. Our system thus offers a high degree of freedom and diversity for the creation and use of currencies, while maintaining a strong and consistent value proposition for the native currency.

2.1 References and footnotes

Theorem 1 (Solidity Language) *Rethereum uses the Solidity programming language to enable our programmable blockchain.*

Solidity Team, https://soliditylang.org/

```
A programmable currency is a type of digital money that can be customized and
programmed to perform various functions and transactions. However, it does not
have the ability to alter the underlying network, blockchain or native
currency that it operates on. Rather, it works in harmony and compatibility
with these elements, leveraging their security and scalability.
```

3 Rethereum is not Ethereum

$$A \neq B \tag{1}$$

Rethereum, existing in response to problems enabled by Ethereum's centralization, quickly realized and adopted the genius of Bitcoin's decentralist design decisions.

Like `ETH`, `RTH` is a Turing Complete Smart Contract Platform.
Like `BTC`, `RTH` has a miraculous origin, which is impossible to recreate.
Like `BTC`, `RTH` has "no official anything", preventing "official" capture.
Like `BTC`, `RTH` aims to provide a reliable secure base layer and does so by upgrading the protocol conservatively.
Like `BTC`, `RTH` requires constant skepticism in community interactions.

A simple way to understand what Rethereum aims to do is to compare it with the current state of the cryptocurrency world, especially for those who have some prior knowledge of it.

When The Ethereum Foundation decided to forsake the principles of decentralization that attracted many supporters and contributors, it was a regrettable move that also created an opportunity for a new project that would uphold the Original Ethereum Vision.

By switching to proof-of-stake, Ethereum became a centralized system under one authority, which goes against the spirit of cryptocurrency.

4 Proof Of Work Consensus

One of the main differences between Rethereum and Ethereum is the choice of consensus algorithm. While Ethereum is planning to transition from Proof-of-Work (PoW) to Proof-of-Stake (PoS) in the near future, Rethereum is committed to keeping PoW as the core mechanism for securing and scaling the network. In this section, we will explain the rationale behind this decision and the benefits of using a modified version of Ethash, called EthashB3, that leverages the advantages of Blake3 hashing function.

PoW is a well-established and robust consensus algorithm that has been successfully used by many cryptocurrencies, including Bitcoin and Ethereum. PoW requires miners to solve a cryptographic puzzle in order to create new blocks and earn rewards. The difficulty of the puzzle is dynamically adjusted to ensure a stable block time and a fair distribution of rewards. PoW provides a high level of security and decentralization, as it makes it costly and difficult for any malicious actor to attack or manipulate the network.

One of the challenges of blockchain technology is to achieve a secure and decentralized consensus among the network participants. Proof-of-Work (PoW) is a common consensus mechanism that requires nodes to solve complex mathematical problems and compete for the right to append new blocks to the ledger. PoW, however, has some limitations, such as high energy consumption, vulnerability to 51% attacks, and low scalability. A different consensus mechanism that aims to overcome these limitations is Proof-of-Stake (PoS), which does not depend on mining. PoS nodes stake their own coins to validate transactions and receive rewards. PoS improves the efficiency and scalability of the network, and also lowers the environmental impact and the hardware costs of running a node. However, PoS also introduces new challenges, such as the risk of centralization and the lack of incentives for honest behavior. Therefore, many blockchain platforms, such as rethereum, have decided not to adopt PoS on their network.

Rethereum, believes that PoW is a viable and preferable option for achieving security and scalability, especially with some modifications and improvements. Rethereum proposes to use EthashB3, which is a variant of Ethash that replaces the Keccak hashing function with Blake3. Blake3 is a new hashing function that was designed to be fast, secure, and versatile. Blake3 offers several advantages over Keccak, such as:

- Faster performance: Blake3 can achieve speeds of up to 10 GB/s per core on modern CPUs, compared to Keccak's 0.3 GB/s. This means that EthashB3 can process more transactions per second and reduce network congestion.
- Lower memory usage: Blake3 uses only 32 bytes of internal state, compared to Keccak's 1600 bytes. This means that EthashB3 can reduce the memory footprint and bandwidth requirements of nodes and miners.
- Simpler design: Blake3 is based on a single compression function, called Chacha, that is widely used and tested in cryptography. This means that EthashB3 can reduce the complexity and the potential for bugs or vulnerabilities in the code.
- Higher security: Blake3 provides 256-bit security against all types of attacks, including quantum attacks. This means that EthashB3 can ensure the long-term security and integrity of the network.

By using EthashB3, Rethereum aims to preserve the benefits of PoW while mitigating its drawbacks. EthashB3 can offer a higher level of performance, efficiency, simplicity, and security than Ethash, making Rethereum a more competitive and attractive platform for developers and users.

5 On-Chain Innovation

Rethereum is a cryptocurrency that aims to create a long-term stable economy, unlike many other cryptocurrencies that are subject to volatility and uncertainty. One of the ways that Rethereum achieves this goal is by transitioning to a stable inflation emission rate for miners, which is based on the global accepted average of 2.1%. This means that the supply of Rethereum will increase at a predictable and moderate rate, ensuring that the network remains financially secure and sustainable.

Another way that Rethereum fosters innovation and stability is by introducing onchain bonds, which are contracts that allow users to lock up their coins for a fixed period of time and receive a token value percentage as a reward at the end. These bonds can be bought and sold between users, creating a secondary market for long-term investments. Bonds can also be used to inject new capital into the network, which can help balance out the various ways that coins are lost, such as lost wallets, incorrect transactions, theft or death. By offering users an incentive to hold their coins for longer periods of time, Rethereum can increase the demand and value of its currency.

6 The Team

Rethereum is a project that aims to be owned and run by the community. The initial team of 3 developers is only a temporary facilitator of the development and launch of the blockchain. The ultimate vision is to have a decentralized and democratic governance system, where changes, ideas and scrutiny are conducted by the users of the blockchain. We believe that this is the best way to ensure the security, innovation and sustainability of Rethereum.

Moreover, a community ran blockchain is more secure and has everyone's interests at heart, as it prevents any single entity from controlling or manipulating the network. By empowering the users, we hope to create a fair and transparent platform for decentralized applications and smart contracts.

Additionally, this also prevents a single government's laws from being imposed on the network, as the network is governed by its own rules and consensus mechanisms. This way, Rethereum can maintain its autonomy and independence, while also respecting the diversity and freedom of its users.

7 Road map

Rethereum's vision is to create a blockchain platform that offers security, sustainability and decentralization for the cryptocurrency community. The platform's currency emission model is one of the key features that supports this vision. The model regulates the supply of RTH tokens, which are the native currency of Rethereum, by reducing the emission rate every few years.

- The initial rate is 4 RTH per block
- Will decrease to 3 RTH after 4 years,
- Will decrease to 2 RTH after 6 years
- Will decrease to 1 RTH after 9 years.
- At this point, the transition to a stable inflation rate of 2.1% per year and remain constant.

Another important feature that Rethereum intends to develop after the 9-year mark is a bonds system for the blockchain. This system will enable users to lock their RTH tokens for a certain period of time and earn interest on them. The bonds system will create more demand for RTH tokens and encourage long-term holding. Besides these features, Rethereum's roadmap also covers other aspects such as smart contracts, cross-chain interoperability and governance mechanisms.

8 Issuance Allocation

One of the aspects of Rethereum's currency emission model is the issuance of coins to the foundation wallets. These are special wallets that belong to the initial team of developers and facilitators of the project. The purpose of these wallets is to fund the development, maintenance, and promotion of the network, as well as to reward the contributors and supporters of Rethereum.

The total amount of coins issued to the foundation wallets is 2,100,000 RTH, which represents 1.68% of the total supply after 9 years. These coins are locked for a fixed period of time and soft-locked, which means they need a special crafted transaction to unlock fully. The locking mechanism is implemented by using smart contracts, which ensure that the coins cannot be spent or transferred until certain conditions are met.

For the first 12 months after the network goes live, the foundation wallets will be locked and inaccessible. No transactions involving these coins can be made during this period. Once the locking period ends, the coins will enter a soft-unlock phase, where a final unlock of the funds can be done by invoking the smart contract.

The soft-unlock phase is designed to prevent a sudden influx of coins into the market, which could cause price instability and inflation. It also ensures that the foundation has a long-term commitment and incentive to support and improve the network. The soft-unlock phase also allows for some flexibility and adaptability, as the foundation can decide when and how to use the unlocked coins, depending on the needs and priorities of the network.

The issuance of coins to the foundation wallets is a transparent and accountable process, as all the transactions and balances can be verified on the blockchain. The foundation will also publish regular reports on how the coins are used and allocated, as well as solicit feedback and suggestions from the community. The foundation's goal is to use the coins in a responsible and effective way, to foster innovation, growth, and sustainability for Rethereum.

References

[1] Ethereum Foundation, https://ethereum.org/en/

[2] Ethereum Whitepaper, https://ethereum.org/en/whitepaper/

[3] US Government bonds https://www.investor.gov/introduction-investing/investing-basics/investment-products/bonds-or-fixed-income-products/bonds

[4] Crypto Proof-of-work https://en.wikipedia.org/wiki/Proof$_o f_w ork$