neatio

Whitepaper

written on

February the 17th, 2022

revised April, the 28th, 2022,
revised November 28, 2022,
revised September 19, 2023.

Revision v3.0

www.neatio.net

TABLE OF CONTENTS

[1]. ABSTRACT

One of the earliest attempts at creating a cryptocurrency actually predates Bitcoin[a] creation by about 20 years by a group of developers who attempted to link money to newly-designed smartcards. This may have been the earliest example of electronic cash, which has links to digital currencies as we know them today. Some other attempts to create digital money were made by Wei Dai who proposed an "anonymous, distributed electronic cash system" called B-money[b], Nick Szabo who proposed the first electronic cash with its own PoW[c] (proof-of-work) system and Hashcash[d] which was one of the most successful pre Bitcoin digital currencies. When Bitcoin was developed in 2009, it launched a new generation of digital currencies. Bitcoin differs from many of its predecessors in its decentralized status and its development of blockchain technology. Bitcoin has captured everyone's attention as being the currency of the world and we all love it and appreciate it since it introduced us a new way to transfer value. Satoshi Nakamoto described Bitcoin in the whitepaper as "a purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution" but because of the lack of scalability, slow processing time and expensive transactions, Bitcoin "failed" to be what Nakamoto envisioned 12 years ago. Bitcoin has become more of a "store of value" asset, rather than a decentralised payment system.

[2]. INTRODUCTION

What is Neatio?

Neatio is a decentralized peer-to-peer network based on blockchain technology like Bitcoin and Ethereum[e] which is composed of a main blockchain and multiple derived side-chains with the main focus on exchanging value (payments) fast, secure and inexpensive. Of course the platform is not limited to payments only, since Neatio can also be used by other developers to run their own dApps (decentralized applications) and/or launch their own cryptocurrencies.

Why is Neatio different?

Neatio is built to be an advanced payment solution, powered by state-of-the-art blockchain technologies which make it blazing fast, ultra secure, highly scalable and inexpensive to use. Say goodbye to network congestion and confirmations time, Neatio transactions are executed in real time and once they are included in the next block they are final meaning that in Neatio network there is no need for subsequent block confirmations. This makes it an ideal payment solution for merchants in day-to-day use and also for individuals since we all need things to happen fast in our crazy fast-forward lives that we are living.

[3]. PROOF-OF-STAKE EXPLAINED

Proof-Of-Stake or (PoS) for short is a an alternative newer method of consensus protocol and block generation was created as an alternative to Proof-of-Work (PoW), the original consensus mechanism used to validate a blockchain and add new blocks. The PoS consensus was invented by Sunny King and Scott Nadal and first introduced in Peercoin[f] in 2012. In a PoS network, the coin owners are the ones that verifies and validate entries into a distributed database (blockchain) and keeps the database secure.

However arguably one of the more secure methods of distribution though not as readily available to newcomers just climbing on board a project. This is because PoS uses the coins that a participant owns and is holding to generate a block, thus owning more coins and staking them provides the participant with a higher possibility of generating the next block.

Staking is the act of allowing one's client to remain online in order to support the network by having randomly selected coins become temporarily unavailable while the client forges a block and then compensates the participant with an earned interest on the coins used. This method is considered more secure as if properly distributed the participants will invalidate most any form of attack that abuses hashing power in order to gain control of a blockchain, however one must first obtain coins in order to stake which depending on their worth can be costly and overall a deterrent to the project if this is the only method available.

[4]. BFT CONSENSUS EXPLAINED

The consensus protocol is the core of blockchain to provide agreement services, whose efficiency highly affects the performance and scalability of a blockchain system. Without trusted intermediaries, the parties of blockchain may behave arbitrarily and deviate from the consensus procedures, in which we can literately consider them in a byzantine environment. Blockchain can benefit from many technologies developed for reaching consensus, replicating state, and broadcasting transactions, but in cases that network connectivity is uncertain, nodes may crash or be subverted by an adversary. Though there are many proof-based consensus protocols for blockchain assisting to solve these issues, i.e., Proof-of-Work (PoW) in Bitcoin, they are typically not energy efficient and may cause power starvation. Fortunately, Byzantine fault-tolerant or BFT[g] state machine replication (SMR) offers some opportunities to design consensus protocols that can tolerate arbitrary faults. Under the hood of BFT SMR, it replicates the state of each replica among the replication system. The capacity to tolerate arbitrary faults makes the BFT replicated system a reality when building some practical and critical applications.
Practical Byzantine Fault Tolerant pBFT[h] has been long-termly as a consensus protocol to cope with Byzantine systems, which can tolerate up to a 1/3 of Byzantine faults in a system. One replica, the leader replica, decides the order for clients requests, and forwards them to other replicas, the secondary replicas.

[4]. BFT CONSENSUS EXPLAINED

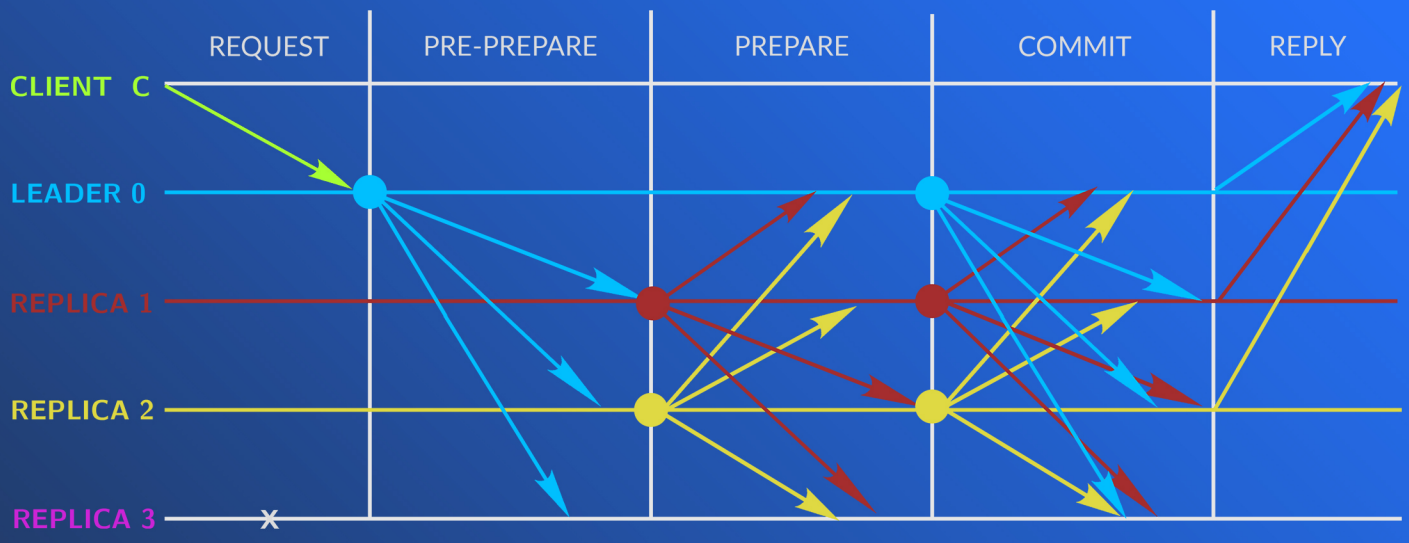

Figure 1.

The three-phase consensus rounds as showed in Figure 1 explained:

A CLIENT C sends a request to invoke a service operation to the primary process 0.
This is the LEADER for this round of consensus.

The LEADER broadcast the request to other other processes, 1, 2 and 3.
These processes are called replicas.

Replicas execute the request and send a reply to the CLIENT .

The client waits for f+1 replies from different replicas with the same result;
This is the result of the operation.

The pBFT protocol guarantees that safety is maintained even during periods of timing violations, because progress only depends on the leader. On detecting that the leader replica is faulty through the consensus procedure, the replicas trigger a view-change protocol to select a new leader to coordinate the consensus procedure. The leader-based protocol works very well when the number of participating replicas are small, but, it is subject to scalability issues. In general, pBFT is regarded as the baseline for almost all BFT protocols published afterward. Even though many pBFT-like solutions are proposed in the literature, most of them are still subject to scalability issues, which cause them not to fit some large-scale mainstream distributed systems, such as public blockchain systems.

[5]. NEATIO KEY FEATURES

- One second block time; enforced by the consensus protocol to have a constant block generation and reward our validators with a constant amount of NIO;
- High scalability with no confirmation time; Neatio blockchain can handle more than 1,000,000 transactions per second.
- Dynamic block size; every block can stretch up to 20 MB when more transactions have to be executed at the same time.
- Smart contract support; Based on EVM, Neatio blockchain is compatible with Solidity and Ethereum smart contracts.
- Side-chains implementation for limitless scalability.
- Eco-friendly; Neatio validations doesn't need specific mining equipment and huge amount of electricity to secure the chain like in PoW blockchains (i.e Bitcoin).

[6]. NEATIO TECHNICAL DETAILS

- Hashing algorithm: SHA256
- Signing algorithm: Secp256k1
- Proof-of-Stake with custom pBFT consensus
- Max supply that will ever exist: 100,000,000 NIO
- Decimals: 18; Smallest unit is 0.000000000000000001 NIO

[7]. NEATIO CONSENSUS EXPLAINED

NEATCON, the custom implementation of the pBFT consensus in the Neatio network is based on the classic pBFT protocol (see section 4), with 2 major improvements:

1. BLS[i] signatures; Boneh–Lynn–Shacham signature keys, improves nodes communication.

2. RLS validation; Random Leader Selection by using a verifiable random function or VRF[i].

The pBFT consensus is a protocol with three phases: pre-prepare, prepare and commit. In phase prepare and commit, each validator has to broadcast its vote for the proposed block. Upon receiving 2f+1 commit votes, each validator finalizes the block. Due to the broadcasting of votes, the complexity of communication grows as the square of the number of nodes, O(n^2). To reduce this, NEATCON establishes a leader for each voting round to collect votes from all validators. In addition, NEATCON adopts BLS threshold signatures to achieve linear communication. An (n,t)-threshold signature on a message m is a single, constant-sized aggregate signature that passes verification if and only if at least t out of the n participants sign m. Note that the verifier does not need to know the identities of the t signers. Each collector derives an (n,2f+1)-threshold signature after collecting 2f+1 votes. The threshold signature can be seen as a single signature with constant size. After that, the collector broadcasts the threshold signature and each validator can confirm that more than 2f+1 validators have voted for the proposed block via verify threshold signature. In classic pBFT, two rounds of voting are used to guarantee the safety and liveness of protocol. However, in NEATCON, a single round of voting achieves this without losing safety or liveness. And as each vote for the current block specifies the hash of the previous block, each vote is the confirmation for the previous block as well. Hence, the vote for the current block is the prepare-vote and commit-vote for the current block and the previous block at the same time. If more than 2f+1 votes for the current block are collected by a validator, the previous block is finalized at once. Therefore, each block is finalized after just two rounds of voting which ensures the safety of the network.

Similar to pBFT, the view change sub-protocol of NEATCON is triggered when the validators cannot reach consensus in a single round. This can be due to an asynchronous network (e.g., when more than 1/3n nodes are offline), or the presence of malicious collectors/leaders. NEATCON handles a view change with the Linear View Change (LVC) algorithm. The essence of LVC is that the leader of the next round sends its highest commit certificate instead of all commit certificates, which reduces transmission volume during a view change by a factor of O(n). In pBFT or tendermint, each leader is decided in a round-robin scheduling which can be predicted by the adversary. NEATCON avoids this situation by selecting its leaders randomly, using a VRF (verifiable random function). A VRF is a pseudo-random generator whose output is verifiable (i.e., on whether a given number is indeed the output of the VRF), random, uniformly distributed, and unpredictable beforehand. With random leaders, the leader of the next round is unpredictable and the adversary can not attack the leader in

[8]. NEATIO TOKENOMICS

Since Neatio total supply is capped at 100,000,000 NIO, the minting will last for 10 years and will end of year 2033 with a yearly inflation starting from 5.11% as seen below:

YEAR	SUPPLY	INFLATION	PERCENT
2023	67,933,310	867,350	5,11 %
2024	71,402,710	3,469,400	4,86 %
2025	74,872,110	3,469,400	4,63 %
2026	78,341,510	3,469,400	4,43 %
2027	81,810,910	3,469,400	4,24 %
2028	85,280,310	3,469,400	4,07 %
2029	88,749,710	3,469,400	3,91 %
2030	92,219,110	3,469,400	3,76 %
2031	95,688,510	3,469,400	3,63 %
2032	99,157,910	3,469,400	3,50 %
2033	100000000	2,602,050	3,38 %

[9]. NEATIO PROOF-OF-STAKE

Some more technical details

The block reward is aproximatelly 9504 NIO per day;
Epoch duration is approximately 1 (one) day or 86400 blocks;
Total epochs number is 3650 (the reward per block is paid);
Total time the reward per block will be paid is 10 years

Validators requirements

System 8 CPU, 16 GB RAM, 500 GB SSD, Static IP;
Cloud (VPS) is strongly recommended;
Collateral: 1,000,000 NIO.

[10]. PROJECT OBJECTIVES

Neatio is trying to revolutionize the traditional payment system which is inefficient, unsecure and expensive to use. Our platform is bringing the latest blockchain technologies to masses and the end user can benefit from the advantages of our platform in terms of decentralization, speed, security, privacy and costs.

Decentralization

Even thought a centralized payment system have very high security requirements for their central servers at any time f a security vulnerability can be exploited and the hole network is at risk and can collapse. Many times the users can't use the network anymore leaving them without access to their funds or worse have their funds stolen. On Neatio platform the network is secured by many servers spread all around the globe and the transactions are executed by the network validator nodes, making the Neatio payment system available 24/7, 365 days a year.

Speed

In terms of speed no traditional payment system can match Neatio, not even Visa, PayPal or Skrill. Here we don't have anything to compare with since not even the top blockchain networks or platforms out there like Bitcoin, Litecoin, Monero nor Ethereum, Cardano, can match Neatio in terms of speed and scalability. Neatio blockchain can handle more than 1,000,000 transactions per second with a confirmation time of 1 second thanks to the custom pBFT consensus, NEATCON.

Costs

The costs are negligible, every transaction fee is 0.0001 NIO. Which in terms of USD is free. In comparison with bank transfers, WesternUnion, Neatio transactions are basically free. In comparison with Visa, PayPal or Skrill is also negligible, their free transfer fees are not really free as you will find out from the next paragraph.

Privacy

Existing centralized payment systems can collect their users data at will. They can collect many information, and use this data for digital advertising, website analytics and even sell users data to 3rd party companies for money. Why? Do you ever wondered how can a company afford to pay their huge infrastructure costs and maintenance, employees and also making profit if using their services *"is free"*

Like we state in the first part our main focus is on creating an efficient payment system, but our platform is not limited on payments alone, Neatio network can also be used to create new tokens or to run dApps such as DeFi and NFTs on top of it.

[11]. NEATIO 3.0 KEY CHANGES

Neatio 3.0 brings the following network changes:

- Address format changed to custom NIO3 prefixed 32-character
  · new address look: “NIO3xmT7VH9kDx8yog7CmU2fh21NXNF2”

- Coin ticker was changed from NEAT to NIO.

- Maximum total supply was increased to 100 Million NIO;
  · changed from 50,000,000 NIO to 100,000,000 NIO.

- Minimum collateral needed by a Validator was changed;
  · increased from 50,000 NIO to 1,000,000 NIO.

- Low-level punishment for Validators was introduced;
  · offline Validators will be kicked out from the Validators pool;
  · no coins will be lost, no coins will be earned;
  · kicked-out Validators will just need to re-register.

- The network native coin inflation was reduced, hence;
  · APR rewards starts at 10% decreasing linearly to 5%

- Protocol now enforces a block spacing of 1 second;
  · lowered from 1.7 seconds to only 1 second.

- Epoch time duration was changed from one hour to one day;

[12]. DISCLOSURE

The information in our whitepaper is used only for the purpose of conveying information and does not constitute an opinion on the trading of Neatio (NIO) cryptocurrency. Any such proposal shall be carried out under a trustworthy term and with the permission of the applicable securities law and other relevant laws. The above information and/or analysis shall not constitute investment decisions or specific recommendations. The whitepaper does not constitute any investment advice on the form of securities, investment intent or abetting investment. Our whitepaper is not composed nor construed as providing any transaction or any invitation to buy or sell, nor any form of securities or any form of contract or commitment. We express the intention that the user has a clear understanding of the risks of the cryptocurrency platforms. Once the investor participates in the investment, he/she will understand and accept the risk of the project and be willing to bear all the corresponding results or consequences. We expressly disclaims that Neatio (NIO) will not bear any direct or indirect damages resulting from any participation in our project, including this whitepaper, website and any software and/or materials provided on our websites and social media channels. Please do your own research before making any investment decisions. None of the information in this document constitutes. Cryptocurrency investments are volatile and high risk by nature. Do not invest more than what you can afford to lose.

Also take note of the risk associated with the Ethernet core agreement since Neatio (NIO) is based on the Ethernet protocol development, any failure, unpredictable functional problems, or attacks that occur in any Ethernet core protocol can cause Neatio (NIO) or our applications to stop working or can behave in an unpredictable manner. The risk associated with using third party apps, websites and/or tools that can obtains the user's login credentials or private keys will be possible to directly control the user's funds. In order to minimize the risk, the user must protect its electronic devices to prevent unauthorized access requests from accessing the device content. The risk that our applications and/or products may not meet the expectations of users since our applications and/or products are currently in the development phase and may be subject to major changes before the release of the official versions. Phishing and/or Theft risks associated with hackers, other organizations or even countries have the potential to attempt to interrupt our applications and/or functionality in any way, including service attacks, Sybil attacks, malware attacks, or consistent attacks. The risk of uninsured losses since the coins stored in your account is not insured like the money stored in the bank accounts or any other financial institutions. The risk of the presence and/or application failure, meaning that our websites and/or platforms may break down due to various reasons, and therefore may not be able to provide the normal expected services.

[13]. DISCLAIMER

The information contained in the whitepaper is provided for informational purposes only and may not be entirely accurate or up-to-date. While we strive to ensure the accuracy and reliability of the information presented, we cannot guarantee its completeness or correctness. The content within the whitepaper is subject to change without notice, and we do not assume any responsibility or liability for any errors, inaccuracies, or omissions that may occur.

Readers should exercise their own judgment and seek professional advice when necessary, as the information in the whitepaper may not be completely accurate or comprehensive.

[14]. REFERENCES

a) Satoshi Nakamoto. “Bitcoin: A Peer-to-Peer Electronic Cash System” https://bitcoin.org/bitcoin.pdf. Accessed February 17, 2022.

b) Wei Dai. "B-money.” http://www.weidai.com/bmoney.txt" Accessed February 17, 2022.

c) Nick Szabo. “PoW. Bit Gold” https://unenumerated.blogspot.com/2005/12/bit-gold.html” Accessed February 17, 2022.

d) “Hashcash” http://www.hashcash.org/ Accessed February 17, 2022.

e) “Ethereum” https://ethereum.org/en/developers/docs/intro-to-ethereum/. Accessed February 17, 2022.

f) Sunny King, Scott Nadal, “PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake”. https://www.peercoin.net/whitepapers/peercoin-paper.pdf Accessed February 17, 2022.

g) Gang Wang, “SoK: Understanding BFT Consensus in the Age of Blockchains” https://eprint.iacr.org/2021/911.pdf. Accessed February 17, 2022.