Nyzo: a high-efficiency blockchain

nyzo.co

Preface

Nyzo is an open-source, highly decentralized, democratic, and highly efficient blockchain. The block time is seven seconds, and the system scales well to high transaction volumes. This is not like most of the new coins you see: this is not a derivative of another project, and it is not just a few new features or a slight design change from other projects. This is all-new code, built from the ground up to be the most efficient, most democratic, easiest-to-use cryptocurrency in the world.

Terminology and symbols

Coins in this system are called “nyzo” (plural “nyzos”). The prefix for a nyzo is the mathematical intersection symbol, ∩. So, “5 nyzos” would be written as “∩5.” The smallest unit of measurement is the micronyzo. A micronyzo is 1/1,000,000 of a nyzo. The prefix for a micronyzo is the lowercase Greek letter mu, µ. So, “15 micronyzos” would be written as µ15. To avoid ambiguity and to eliminate rounding issues, all transactions are handled at the programmatic and blockchain levels in terms of micronyzos, and fractional micronyzos cannot be specified anywhere in the system.

Several “edges” are discussed in this system. The “frozen edge” is the highest block

that a verifier has agreed it will never change, and the consensus mechanism is built to extend the frozen edge as quickly as possible while ensuring that no two verifiers acting in good faith ever freeze different blocks at the same level. The “trailing edge” is the lowest block that was necessary to determine the state of the frozen edge, and the “retention edge” is the lowest block for which a verifier will service normal requests. The frozen edge and trailing edge are precisely defined based on characteristics of the blockchain, while the retention edge is an arbitrary buffer behind the trailing edge that is useful in bootstrapping new verifiers.

Proof of diversity

The proof-of-diversity blockchain uses analysis of verification cycles to establish the authoritative form of the blockchain. This is not proof-of-work, and it is not proof-of-stake. It is a totally new proof system that relies on diversity of participation for strength. While proof-of-diversity has its own unique concerns that must be addressed to ensure integrity of the blockchain, it is immune to many of the attacks and problems inherent to proof-of-work and proof-of-stake systems, and it is significantly more efficient.

The basic concept of proof-of-diversity is simple. Verifiers take turns producing blocks in a circular order. Some simple rules ensure that verifiers are neither added to nor removed from that circular order too quickly. In order to produce a believable forgery of the blockchain for any meaningful amount of time, an attacker would need to obtain more than half of the private keys of verifiers currently working on the blockchain.

For any block in the blockchain, the verification cycle of that block is defined as the

longest list of blocks, ending with that block, that contains no more than one instance of each verifier. Consider the following blockchain, where the number is the block height and the letter is the verifier:

```
20A, 21B, 22C, 23A, 24B, 25C, 26A
```

In this blockchain, the verification cycle of block 26 contains blocks 26, 25, and 24. The cycle does not contain block 23, because verifier A is already in the cycle at block 26. The verification cycle of block 25 contains blocks 25, 24, and 23. The cycle does not contain block 22, because verifier C is already in the cycle at block 25.

If a verifier is new to the chain, the same definition holds. To illustrate, we add verifier D at block 27:

```
20A, 21B, 22C, 23A, 24B, 25C, 26A, 27D
```

The verification cycle of block 27 is blocks 27, 26, 25, and 24. The cycle does not contain block 23, because verifier A is already present at block 26.

The previous cycle of the block is the cycle immediately before the current cycle. The previous cycle of block 27 in this example would contain blocks 23, 22, and 21, but not block 20, as verifier A is already present in that cycle at block 23.

A “new” verifier is defined as any verifier other than the last verifier of the previous cycle. An “existing” verifier is defined as the last verifier of the previous cycle. If an existing verifier misses a cycle, it will be considered a new verifier the next time it verifies a block.

Building on these definitions, we declare two rules to secure the proof-of-diversity blockchain.

Proof-of-diversity rule 1: After the first existing verifier in the blockchain, a new verifier is only allowed if none of the other blocks in the cycle, the previous cycle, or the two blocks before the previous cycle were verified by new verifiers.

This rule exists to ensure that attackers cannot gain control of the chain by quickly introducing verifiers that they control. The addition of the two blocks before the previous cycle is to avoid clustering new verifiers in the chain.

Proof-of-diversity rule 2: Past the Genesis block, the cycle of a block must be longer than half of one more than the maximum of the all cycle lengths in this cycle and the previous two cycles.

This rule exists to ensure that the majority of the verifiers who are verifying the blockchain cannot be excluded by attackers who are trying to take control of the blockchain. In order to control the direction of the chain, one must control more than 50% of the current active verifiers. The blocks in this and the previous two cycles are considered to avoid divergence at opportunistic moments for verifiers that are clustered around certain parts of the chain.

The metric calculated in this rule cannot increase from one block to the next unless the cycle length also increases from one block to the next. This is important because it ensures that every block that passes this rule can be extended indefinitely.

These are the only two blockchain rules, and together they guarantee that, starting at any point in the blockchain, one must control more than half of the active verifiers to

continue to produce a valid version of the blockchain. Unlike proof of work, which can be manipulated at will by anyone in possession of sufficient computational resources, proof of diversity requires active participation in a particular blockchain to have any influence on that blockchain.

Consensus techniques

Proof of diversity provides a mechanism for determining which version of the blockchain the mesh agreed to produce, but we also need a mechanism that the mesh can use to come to agreement on which version of the chain it will continue to extend.

Scoring

Each block has a score based on the verifier that signed it. A lower score is better than a higher score. At each height, an incremental score is calculated relative to the block at the previous height, and the total score of a block is the sum of all incremental scores back to the frozen edge.

For a block signed by an existing verifier, the incremental score is zero plus four times the difference between the previous block's cycle length and this block's cycle length. If the verifier is not active in the mesh, five is added to the incremental score.

For a block signed by a new verifier, the incremental score is negative six plus four times the verifier's position (zero-indexed) in the new-verifier vote total list. Twelve is added to the score of a new verifier not present in this list, which is limited to a maximum size of three.

Voting

A verifier may change its vote for a block several times. Votes are timestamped to prevent replay attacks of old votes.

If a block has a score less than 0, a verifier may vote for it immediately after freezing the previous block. Otherwise, it must wait 2 seconds minimum plus 20 seconds for each point that a block has above 0. So a block with a score of 0 can be voted for after 2 seconds, while a block with a score of 4 can be for after 82 seconds.

If the leading block in a verifier's local tabulation has more than 50% of the vote, the verifier changes its vote to that block if the verifier is allowed to vote for that block based on its score. If the leading block in a verifier's local tabulation does not have more than 50% of the vote, the verifier changes its vote to that block if the verifier was allowed to vote for that block more than 10 seconds ago.

If neither of these conditions is true, the verifier votes for the block with the lowest score if it is allowed to cast a vote based on that block's score. Until such a block exists, the verifier waits to cast a vote.

Vote tabulation and freezing of blocks

In tallying votes, only votes from verifiers in the frozen edge's verification cycle are counted. A block is frozen if the votes for that block exceed three-fourths of the size of the verification cycle in two subsequent vote tabulations calculated at least 0.5 seconds apart.

At the three-fourths threshold, more than half of the cycle would have to maliciously send different votes to honest verifiers in order to cause a divergence of the chain,

assuming the worst case in which the remaining honest verifiers are split evenly on which block to freeze.

Transaction fees

All transactions incur a 0.25% fee. This fee is split evenly among the verifier of this block and the verifiers of the previous nine blocks. For blocks before block 9, the fee is split evenly among the verifier of this block and all previous blocks. Transaction fees that cannot be divided evenly are rounded down to the nearest micronyzo, and the remainder is rolled over to the next block.

Maintenance fees

Every account except 0000000000000000-0000000000000000-0000000000000000-0000000000000001 is charged a fee of µ1 every 500 blocks from its creation for as long as it has a balance greater than 0. This fee is intended to combat intentional overwhelming of verifiers through creation of many small accounts, and it is a negligible amount for legitimate accounts. The number of blocks per year is just over 4.5 million, and this results in maintenance fees of approximately ∩0.009010 per year per account.

Joining the mesh

When a Nyzo verifier is started, it asks other verifiers for information on the current state of the blockchain. The location of verifiers are specified in the file /var/lib/nyzo/production/trusted_entry_points. In the initial distribution, the Nyzo verifiers (verifier0.nyzo.co through verifier9.nyzo.co) are listed in this file, but it may be modified at any time.

Only one verifier is allowed to be run at each IPv4 address. As nodes take very little computational power, a single system could otherwise run many instances of the Nyzo software and take a disproportionate share of transaction fees. This will prevent some users from running Nyzo verifiers in situations with shared public IP addresses (dorms, offices), but that is an acceptable limitation to ensure fairness in transaction verification. Also, this limitation does not prevent multiple Nyzo clients at an address.

Two mechanisms are in place to enforce the IPv4 address restriction. First, in the list of verifiers waiting to join the verification cycle as a new verifier, any verifier changes at an address cause that address to be demoted to the end of the queue. Second, when an existing verifier produces a block, a penalty score is applied if that verifier is not currently listed as active in the mesh. To prevent shuffling of a large set of verifiers over a smaller set of IP addresses, the verifier at an IP address is only allowed to be reassigned at a time interval slightly larger than the time interval of the current verification cycle length. So, attempts to circumvent the IPv4 address restriction will result in difficulty joining the cycle as a new verifier and will risk being removed from the cycle as an existing verifier.

Genesis block

The Genesis block starts the Nyzo blockchain and generates all coins for the system. It contains a single type-0 transaction that transfers ∩100,000,000 to address 64afc20a4a4097e8-494239f2e7d1b1db-de59a9b157453138-f4716b72a0424fef.

Democratization

To ensure complete democratization, we will deactivate all of our verifiers (verifier0.nyzo.co through verifier9.nyzo.co) within 12 months of the Genesis block. We had originally planned to stop committing code to the official Nyzo repository as well, continuing our work on forks or other implementations of Nyzo without revealing our identities as original developers of Nyzo. We had planned this because we have seen too many open-source projects that start out with great ideas from a small group or an individual, only to be held back later due to deference to that group's or individual's opinions instead of the better ideas of the community at large. Open source doesn't live up to its full potential when only one team controls all the important decisions.

However, we now feel that stopping contributions the official repository so soon after the start of the blockchain would be harmful to the progress of the project and would feel like abandonment of the project on our part. We still hope that competing implementations of Nyzo will be developed, and the democratic nature of Nyzo means that we have no control over which implementation or implementations become dominant in the cycle. So, we plan to continue contributing to the official Nyzo repository indefinitely, and we will let the community decide whether they want to use

our implementation.

While the proof-of-diversity blockchain has some rules that must be followed, these rules are incredibly simple, and all of the consensus rules can be modified or replaced without jeopardizing the proof of diversity. At any point in time, the decisions of the active verifiers in the current verification cycle determine the direction of the blockchain.

Sustainability

While we all want to see cryptocurrencies succeed, many investment experts think that most cryptocurrencies will eventually be completely valueless. Unlike physical assets with intrinsic scarcity or shares of companies or fiat currency with enforced scarcity, anyone can take the source code of an existing cryptocurrency, make some improvements to it, and issue a new cryptocurrency without contributing any value back to the original cryptocurrency.

Of course, as an open-source project, anyone will be able to use the Nyzo source to create a new blockchain, and we think that is a wonderful thing. However, we also want for the Nyzo cryptocurrency to have long-term, sustainable value. While a particular cryptocurrency may not typically have an intrinsic value, the community and the technology surrounding the currency do have such value. We think it is only fair to tie the value of the original currency to the value of the community and the technology, and we think this is the best way to ensure that Nyzo will maintain its value in the long run.

Our proposal is simple: if technological advancements render the current Nyzo

system or blockchain obsolete, and a new blockchain needs to be released, all the coins in that system should be derived from original Nyzo coins. There should be no mining and no generation of new coins that are not tied to original Nyzo coins. This does not mean that all future generations of Nyzo will have to have the same number of coins as the current generation. For instance, if the second generation has 200 million coins instead of 100 million, then each first-generation Nyzo coin that is traded in will be rewarded with two second-generation Nyzo coins.

The sustainability program will work as follows. Any coins transferred to address 0000000000000000-0000000000000000-0000000000000000-0000000000000001 are transfers to the next blockchain. The next blockchain will periodically inspect the previous blockchain for transfers to that address and will generate appropriate coins in the next blockchain corresponding to the source identifier and amount of the transaction on the previous blockchain. Democratic processes would govern all of these decisions, with the current cycle of each generation serving also as the Genesis cycle of the next generation when the next generation of the blockchain begins.

The sustainability address (0000000000000000-0000000000000000-0000000000000000-0000000000000001) is the only address that is not charged account maintenance fees. All coins transferred to this address are permanently removed from use in this blockchain.

While this method of transferring assets to the next-generation blockchain does impose an additional implementation complexity on the next-generation blockchain, such is a small price to pay for continuation of blockchain assets beyond obsolescence of the technology that originally created those assets. Applying this transitively, we can imagine a fifteenth generation of Nyzo enabling global commerce 200 years from now, with every last coin in that system having a lineage traceable

back to the Genesis block of the original Nyzo blockchain.