PARiBU NET

Whitepaper 1.0.0

02 February 2022

Abstract

Paribu Net aims to create a new performance-oriented, eco-friendly, and business-focused blockchain architecture with the support of the underlying Proof-of-Authority (PoA) and Delegated Proof of Stake (DPoS) based consensus algorithms, internally referred as Bouleuterion consensus mechanism. Paribu Net is created to connect people and organizations providing new ways of communicating and cooperating with a smooth and reliable data transition. It is important to highlight that Paribu Net will follow the idea of decentralization by introducing a secure, reliable, and trustless transaction network. Paribu Net aims to achieve significantly low transaction fees for users. Paribu Net also supports EVM-based smart contracts to be able to develop decentralized applications such as DeFi, NFT, gaming, metaverse, and domain naming systems.

Contents

Mission

To increase the economic growth by connecting people and providing new ways of communicating and cooperating with a smooth and reliable data transition.

Vision

To be one of the best blockchain platforms as a universally accessible infrastructure in the multi-chain environment. We believe it is a fundamental right to control your asset, data, and identity. Also, decentralized systems are very important in creating a more reliable, secure, efficient, and scalable information society for everyone. To accomplish these goals, we are accelerating this transition utilizing these decentralized systems as they are the most suitable infrastructure for a fully and resilient connected cyber space. We aim to contribute to the progress of the world in this direction. We will achieve this by developing a fast, secure, reliable, publicly verifiable, and robust blockchain platform that is compatible with the most used blockchains in the public network.

1. Introduction

Blockchain technology has been gaining significant attention during the last few years. It can potentially transform the digital space by means integrating data and asset simultaneously due to its public, decentralized, immutable, and append-only ledger. All records in the ledger are secured by cryptographic rules which make it more secure and tamper-proof by removing single-point-of-trust. Industries have been looking for new ways to adapt their products with the blockchain technology for several reasons like cost-efficient asset management and reliability through transparency. This requires the development of new technologies that simultaneously realize various features such as storage, privacy, bandwidth, and efficiency. In 2008, Satoshi Nakamoto opened the gates of a new financial model. Communities and companies have developed several new architectures, consensus mechanisms, and secondary technologies to advance the state-of-the-art digital asset management space and provide new real-life scenarios by means of improving security (through decentralization) and scalability (e.g., storage, computation, transaction per second (tps)).

Scalability and decentralization are the most important challenges of the blockchain technologies today. Most blockchain platforms like Bitcoin and Ethereum have currently high transaction fees, insufficient tps rate, and therefore, unfortunately may not fit to all the business models. Several different projects exist in the global network, however none of them is ready for mass adoption to happen in the international business model. To fill this gap in the technology, Paribu Net aims to provide a scalable, low transaction fee, reliable, trustless, robust, and secure blockchain network that can support various business models.

Paribu Net is the first step of our worldwide community vision, and it is the most important proof of our passion for the development of the community. It is a business-oriented smart contract architecture in a sustainable network. In summary, it aims to support the following features for the community:

• **Quick finality and low latency:** Quick block finality is a core development target for most of the blockchain projects. There have already been several blockchains proposed focusing on the performance. In this respect, Paribu Net aims to improve the existing platforms by means of an eco-friendly, decentralized, and fast consensus methods for the quick finality of the transactions.

• **Decentralization with high throughput:** High throughput is also an important challenge for public decentralized networks (of course as well as centralized systems). Paribu Net will be optimized for the best throughput rates without sacrificing decentralization and transparency of the network. The underlying decentralization and trustless structure enhance reliability to the network.

• **Low transaction fees:** Due to the underlying high throughput, Paribu Net aims to provide much lower transaction fees compared to other platforms.

• **Robustness:** Paribu Net will support the latest standards and most secure cryptographic libraries for the robustness of the underlying network to protect the chain against all types of potential attacks.

• **Highly scalable:** Scalability of decentralized networks is one of the most challenging problems today. Keeping the ledger on many different locations and updating it in a synchronous manner may lead to unscalable networks. Paribu Net aims to provide a more scalable chain with a better node architecture allowing different use-cases to be implemented easily.

• **Accessible:** Paribu Net will be a public and permissionless where anyone will be able to participate to the network at any time. The main characteristics of the blockchain will be transparency and open source.

Overall, the main motivation of Paribu Net is to provide the most adopted and dominant network as the world's universally accessible infrastructure and to allow any business model to be implemented easily.

2. Background

In this section, we present the necessary cryptographic primitives and blockchain basics to be able to describe the technical features and potential functionalities of Paribu Net.

2.1 Cryptographic Algorithms

2.1.1 Hash Functions

Let

$$H: \{0,1\}^* \rightarrow \{0,1\}^k$$

be a cryptographic hash function that maps any data of any size to a fixed size k. The output is also known as *Hash Value*. Secure cryptographic hash functions must basically meet the following properties:

• **Pre-Image Resistance (One-Wayness):** Given an n-bit string y, it should be computationally hard to find an x such that $H(x) = y$.

• **Collision Resistance:** It should be computationally hard to find two distinct strings x_{-1} and x_{-2} such that $H(x_{-1}) = H(x_{-2})$.

• **Second Pre-Image Resistance:** Given x_{-1} it should be computationally hard to find x_{-2} such that $H(x_{-1}) = H(x_{-2})$.

Cryptographic hash functions are the most basic and known tools of modern cryptography. These algorithms are essential in the blockchain space as it ensures the immutability of the chain, is used in digital signatures, and is a pillar of Proof-of-Work (PoW). Both SHA256 [24] and SHA3 [14] (also known as KECCAK) are the most widely used secure hash functions and will also be supported on Paribu Net.

2.1.2 Digital Signatures

Cryptographic signatures are the most critical components in the blockchain space where they are used to prove ownership of an address without exposing the private key. This primitive has an important role in account management without having to trust a central authority. Public keys are used to receive funds while private keys are used to digitally sign transactions. In order to spend the funds, the signature can be validated against the public key without revealing the private key. Furthermore, crypto wallets, on a very high level, are applications to access funds, manage keys and addresses, track balances, create and sign transactions.

ECDSA (Elliptic Curve Digital Signature Algorithm) [21] is the most widely used elliptic curve digital signature algorithm in both the traditional systems and blockchain space. The algorithm provides a high-level cryptographic security with a shorter key length to ensure that funds can only be spent by their rightful owners. They consist of a public and private key pair to control access to crypto funds. Ethereum 2.0 has been using Boneh–Lynn–Shacham (BLS) signature scheme [17] due to its aggregation which enables secure MultiSig capabilities with a much lower memory requirement. Similarly, EdDSA (Edwards-curve Digital Signature Algorithm) [22] is also another digital signature algorithm which is widely used in the blockchain space. Due to its wide adoption in blockchain technologies, Paribu Net will initially start with ECDSA signatures but will keep working to adopt other signature algorithms, especially BLS and EdDSA.

2.1.3 Distributed Random Number Generator

Random number generation is an important part of validator selection process, as described in Section 3. In a decentralized network, majority of the honest participants must be part of the number generation process to generate a secure and reliable random number. However, calculation of a random number in a decentralized network is not trivial. A classical mistake could be to generate a random value on-chain by computing block hashes, block difficulty, or timestamps. The challenge here is that these values may not look random in case of corrupted validator(s).

• **Randao:** Randao is a blockchain-based verifiable random number generator. It is basically a smart contract that defines participation rules of random number generation process. All participants wishing to participate in the random number generation process must create and submit a transaction to the Randao smart contract. After participants create their transactions, Randao generates a random number in the desired range with the necessary input operations.

• **Verifiable Delay Functions (VDFs):** VDFs have been recently become popular in Proof-of-Stake (PoS) based blockchains to be able to get an entropy for a validator and committee selection [16].

Paribu Net will use Randao smart contract which is discussed in Section 4.3.1, providing detailed implementation details. In the future, Paribu Net aims to support VDFs as well.

2.2 Blockchain Basics

2.2.1 Peer-to-Peer Networks

Peer-to-peer (also known as decentralized) networks, disrupting the current centralized models, are organized in a distributed way to allocate hardware and software resources to each node in the network [12,26]. The most important benefit of each node of a decentralized network is to act as a separate autonomous authority with independent decision-making power on how to interact or not with other nodes. These kinds of networks also distribute decision-making and workload functionality among connected nodes. They also offer a unique potential to support social fairness, information accessibility, and security combined with business innovation. Decentralized networks are the core networking protocol of blockchain architecture which has a shared database (known as a distributed ledger) across the network where information cannot be modified with once stored and verified while offering increasing security, and universal verifiability and transparency. The ledger of transactions is replicated and distributed across the entire network nodes. Each block in the chain contains a series of transactions, and each time a new transaction occurs on the blockchain,

a record of that transaction is added to each participant's ledger. The decentralized database managed by multiple participants is known as Distributed Ledger Technology (DLT).

Consensus models allow us to secure the underlying blockchain networks by maintaining consistency across the shared state of the nodes (e.g., PoW, PoS, PoA, Proof-of-History (PoH), Byzantine Fault Tolerance (BFT), Practical BFT (PBFT), Proof-of-Activity (PoA), Proof-of-Capacity (PoC)). The main idea was to eliminate the central authority and create a secure transaction network with honest nodes. The honest nodes that make transaction validation need to hold the total majority of the network and the validation process is also known as mining. In PoW-based blockchains, the power represents the total computational power of miners in the network. Each transaction is verified and put into a block and broadcast by miners. Every time this process takes place, a new block is added to the chains of blocks where the transactions become immutable and verifiable.

2.2.2 Permissionless Blockchain: Ethereum

Ethereum [2,3, 29] is the first blockchain providing Turing complete programming language to develop smart contracts by means of state machines created in all transactions. Thanks to this vision, Ethereum has gained a lot of attention in a short time and built a massive community [3]. Ethereum Improvement Proposals (EIP) and Ethereum Foundation are currently working as the decision-makers of this platform [10]. Ethereum currently uses the PoW consensus model, but the community and Ethereum Foundation invest a great effort to shift to the eco-friendlier and more optimized PoS consensus model [2]. With this effort and efforts shown by other projects, we can openly see that more optimized and eco-friendly consensus models will be the focus of the business side of blockchain technologies. The other important feature of Ethereum is that the project has a large and powerful community. Developers of the Ethereum Foundation and Ethereum community strive to keep Ethereum up to date and secure. This feature makes Ethereum and sub-Ethereum networks a very good option for future blockchain implementations.

• **Ethereum Virtual Machine:** Ethereum Virtual Machine (EVM) [18] is a distributed Turing complete virtual machine that allows Ethereum users to run smart contracts and develop DApps. Ethereum is mainly defined as a protocol for executing a virtual computer/machine inside the distributed network, and this distributed virtual computer is known as EVM. It allows smart contracts working on top of this virtual computer network and all the processes can be monitored publicly thanks to the open nature of the blockchain network. EVM also provides continuous availability of the platform while keeping all the objects of their code safe from modifying. Finally, thanks to Turing complete structure of Ethereum, EVM can basically solve every kind of problem, and this makes it a flexible and strong tool to apply different business models.

Paribu Net uses EVM for every smart contract implementation and specify several gas fees limits to provide better DApp environment for both cooperative users and individual users who wish to run their own smart contract environment.

• **Go Ethereum:** Go Ethereum (Geth) is an implementation of an Ethereum node in the Go programming language. Geth is a command line implementation of Ethereum nodes. It allows user to interact with both main Ethereum network and other private Ethereum networks. The most important feature of the Geth is, it allows us to generate genesis block of one blockchain network and create PoA-based Ethereum network and use all of the capabilities of Ethereum Virtual Machine.

2.2.3 Consensus Mechanisms

Consensus mechanisms allow blockchain networks to maintain their life cycle without the need of a central authority. A consensus mechanism is a fault-tolerant mechanism used in blockchain networks to achieve the universal agreement which is mandatory to accept a single data value or a single state of the network between distributed parties. In blockchain networks, the consensus protocol makes sure that every new block that is added to the blockchain is the one and only version of the truth that is agreed upon by all the nodes in the blockchain.

There are different types of consensus mechanism invented with different aspects.

• **Proof of Work (PoW):** Proof of Work consensus mechanism invented by Satoshi Nakamoto [23] to eliminate central authority and create a data communication network between distributed nodes. A participating node must prove that the work done and submitted by them qualifies for the right to add new transactions to the blockchain. However, this whole Proof-of-Work mining mechanism needs high energy consumption and a longer processing time.

• **Proof of Authority (PoA):** PoA is a center-based consensus algorithm that provides a practical and efficient solution for cooperative blockchain networks. Proof of Authority (PoA) networks does not include any challenge to choose miners [4]. These kinds of network transactions and all other operations are completed by pre-verified *validator* accounts and the nodes which wish to become a *validator* must gain this privilege by the rules of the network. While this structure harms the decentralized nature of blockchain technology, it also provides security and integrity while running an eco-friendly network. PoA consensus algorithms are a good fit for private or centralized blockchain networks where all nodes can see the transactions but may not be able to participate the block creation process [19].

• **Delegated Proof of Stake (DPoS):** In the normal Proof of Stake consensus model, every node with needed native currency in the blockchain network may become a staker and join the block forging process. However, DPoS provides more flexible, efficient, and eco-friendly consensus solutions than PoS. In DPoS, nodes which hold the native currency of the network (stakeholders) have the opportunity to vote for a fixed number of "delegates" (aka witnesses) for validating new blocks. This method is more efficient and democratic than the PoS consensus.

While power-based consensus models such as PoW provide decentralization to the blockchain networks, they are slow and not eco-friendly due to the need of power consumption for the consensus. On the other hand, as we mentioned in other sections, centralized blockchain consensus models such as, PoA provide high-level security and efficient blockchain network, but these consensus models eliminate the decentralization factor of the blockchain technology.

3. System Architecture of Paribu Net

Paribu Net uses the GoEthereum (Geth) project for its main structure by extending with some enhancements such as the underlying consensus mechanism, faster block production, larger block sizes, and low transaction fees. This section presents the main components of Paribu Net.

3.1 Paribu Net Native Coin (PRB)

Paribu Net will have its native coin called PRB. Paribu native coin will allow people to interact with smart contracts for finance, metaverse, gaming, identity management, and supply chain management.

3.2 Entities of Paribu Net

Under this section we present the roles and components we used while we were building the consensus protocol of Paribu Net.

Node: Nodes are the entities which hold the copy of the entire ledger of Paribu Net and keep it updated.

Validator: Validators are the nodes which are ready to produce blocks. There are three types of validators in Paribu Net:

Candidate Validator: All nodes may become candidate validators if they satisfy all the validator requirements.

Main Validator: Main validators are responsible for the management of the network such as block seal, block productions, and execution of proposals. There will be at most 21 main validators in the system.

Standby Validator: Standby validators are waiting to be main validators once the appropriate conditions, e.g., if one of the main validators is jailed or exited. There will be at most 11 standby validators in the system which are sorted according to their voting power. In the case of one of the main validators is jailed, the standby validator which has the highest voting power will be promoted to be main validator.

Staker: Stakers can stake certain amount of PRB coins to candidate validators and receive a portion of block rewards in case the candidate validator becomes a main or standby validator.

- A staker can only invest to one candidate validator during each validator selection period.

- Stakers can claim rewards at any time.

- If a staker is willing to withdraw the staked amount then it will create a request and wait for 3 days ((3 * 24 * 60 * 60) /5 = 51840 blocks, where block period time is 5 seconds) to claim it.

3.3 Bouleuterion Consensus Mechanism

The implemented consensus mechanism of Paribu Net is called Bouleuterion[1] Consensus Mechanism which is the combination of Delegated Proof of Stake (DPoS) and Proof of Authority (PoA). This mixture allows us to provide decentralized selection process alongside with the high performance (e.g., creating a new block in few seconds (≈ 5 secs)).

The consensus of Paribu Net consists of several different roles as described in Section 3.2. The community will select 21 main validators, which are responsible for production and validation of blocks, and 11 standby validators, which will be waiting in the queue to be one of main validators. All the candidate nodes are ranked according to their staked PRB and the total stake amount on the candidates.

Every candidate validator must meet the minimum staking amount and other requirements given in Section 3.4. Any user in the network can invest in any main or standby validators. Therefore, stakers have critical role on the selection of main and standby validators. Candidate validators can offer to share some part of their rewards with their contributors to promote themselves and raise their total staking amount. This competition process will encourage more candidate validators to be selected as a main validator successfully.

1- A bouleuterion known as a council house, assembly house, and senate-house, was a building in ancient Greece which housed the council of citizens of a democratic city-state.

After the selection process, main validators start to produce or validate blocks. The transaction fees in the block are distributed as follows:

- %90 of the fees is equally shared among the main validators.
- The remaining %10 of the fees are equally shared among the standby validators.

Like Ethereum's Clique consensus protocol, the main validators on Bouleuterion consensus model take turns to produce blocks like in the PoA protocol. In the future, these validators are planned to be chosen randomly by using the Randao system contract (see Section 2.1.3). This randomization protocol will allow us to eliminate potential attacks such as a greedy approach during the block generation phase. In addition to this, if any of the main validators act maliciously or fail to generate a block, the slashing contract will take the necessary action as described in Section 4.3.

Above all the features of the Bouleuterion consensus model, the main focus is to create a decentralized decision making and community-driven network. For this purpose, a governance smart contract in Section 4.3.2 has been implemented which allows the community to participate in the decision-making process for the ruleset in the blockchain.

3.4 Validator Requirements and Initialization Phase

Nodes which wish to run a validator in Paribu Net should meet the following requirements:

- Staking should be at least 10,000 PRB coins.
- Validators should meet the minimum hardware and bandwidth specifications. If the verification task cannot be completed, the slashing contract is going to trigger the relevant punishment process.

During the first launch of Paribu Net, there will be a predefined number of validators which will be held on the Genesis stage to maintain and validate the blockchain network. After a certain period, additional candidate validators will be selected by the community through a validator application process with their staking amount.

Each validator is expected to follow the following rules which will be detected through a slashing contract:

- They must complete all the block validation tasks without any latency or interruption.
- They must also be the full node of Paribu Net.
- They must sync with at least 8 other full nodes in parallel.
- In case of any malicious activity or misbehaving condition, a certain amount of the staked coin of the validator will be burned as a penalty.

4. System Contracts and Features of Paribu Net

System contracts are smart contracts to be able to run the general flow of the blockchain network under specific rules. In this section, a detailed description of each system contract will be given.

4.1 Validator Set Contract

This contract validates and stores the nodes that meet the requirements of becoming a validator. Also, the contract can list the main validators and their addresses, the last created and approved block, and classify the blocks produced by specific validator(s). Finally, this contract also carries out the task of selecting the main and standby validators. The contract first makes the necessary selections from the validator staking list which is updated instantly. The candidate validators are sorted according to their vote power, which includes the staking amount of users and validators.

Then, first 21 ranked candidates are selected as main validator which are responsible for block productions. The following 11 candidates are selected as standby validators, which are waiting in the pending queue for being selected as a main validator. This condition happens only in the case of an active validator is jailed or lost its vote power.

4.2 Staking Contract

This contract maintains staking, reward calculations, and distribution of rewards to main and standby validators. This contract periodically updates the rewards earned by the validators and stakers. Bouleuterion consensus mechanism allows decentralization and community involvement. PRB holders, including the validators, can put their tokens ``bonded'' into the stake. Its core logic can be summarized as follows:

1. PRB holders can use their coins to choose a validator candidate or to increase the voting power of a chosen validator.

2. All candidate validators will be ranked by the number of bonded coins on them, and the top 21 will become the main validators. The following 11 validators will be standby validators.

3. Validators can share (part of) their block reward with their stakers. The ratio of reward (from 0% to %100) shares are initially set by the validator and so this ratio can be different for each validator.

4. Validators can suffer from ``Slashing'', a punishment for their bad behaviours, such as double signing and/or instability. Such loss will not be shared by their stakers.

5. There is an ``unbonding period'' for validators and delegators so that the system makes sure the coins remain bonded when bad behaviours are caught, the responsible will get slashed during this period.

The contract itself also collects the validator block rewards and perform the necessary calculations for the reward distribution of each block, allo-

cation of pool reward, and distribute the validator rewards for each address and keep them as a data frame. The validators may claim their rewards via this contract and receive their validator reward via claim transaction. All the rewards will be distributed among all stakers according to the following proportions:

- 90% of the block reward is taken by all the main validators,

- all other standby validators share 10% of the reward parallel proportion of their staking amount and time. If there is no standby validators, this portion will also be distributed among main validators.

Remark: The only difference of unstaking from staking is the waiting time for withdrawal.

4.3 Slashing Contract

Slashing is a part of the on-chain governance to make a punishment for malicious, dishonest, or lazy validators. A slashing contract ensures the needed actions to be taken in case of any malicious activity or any other action causing the interruption of the network. There are two kinds of slashing scenarios:

1. Liveness slashing: Producing blocks timely by the expected main validators in a correct order is known as the liveness property. Paribu Net ensures this property by means of the slashing contract. We note that, due to unforeseen conditions, validators can miss producing blocks in their own turns. However, this may cause bad performance of the network and provides more non-determinism for the block production. In this context, for each validator a counter is used to record the total number of missed blocks in the current day (for every 17280 (=24*60*60/5) blocks). Once the counter is above the predefined threshold for a validator, the validator will be penalized according to following rules.

- If the block missed counter is greater than 20, the validator is punished 1 PRB for every new misses.

• If the counter is greater than 40, the validator is taken into jail for 2 days (2*17280). During these days, the validator cannot produce/validate any block. If there was only one validator left, the jail process would not work due to the sustainability of the system.

• The counter is reset to zero for every 17,280 blocks.

2. Double signing: Anyone can submit a slashing request on Paribu Net with the evidence of double sign, which should contain the two block headers with the same height and parent block, signed by the dishonest validator. If a dishonest validator is caught as doing double signing, the submitter will get 1000 PRB as a reward from the dishonest validator's deposit balance. The remaining balance of the validator is distributed to other validators.

The transaction submission requires slash evidence and cost fees but also brings a larger reward when it is successful. Inside Paribu Net, the following malicious behaviours will be punished accordingly:

• If a Main Validator misses producing 20 blocks in a day, then 1 PRB coin will be subtracted from its deposit for each additional misses.

• If the number of misses is greater than 40, then this validator will be moved to the Jailed List for 2 days and the top of the standby node will be selected as the new Main Validator.

• The Jailed validators are not allowed to seal or produce new blocks since they are not Main Validators anymore.

• After the jailing process (i.e., two days later), the validator will be removed from the Jailed List.

If his/her staking amount is still sufficient to be a Main Validator, then he/she can participate in the selection process to be as a new Main Validator.

If the staking amount is still sufficient to be a Standby Validator, then he/she can be chosen to be a new Standby Validator.

• If a Main Validator produced two blocks with the same parent and the same block height, then this validator will be jailed for 2^64 blocks and all his deposits will be moved to the reward pool.

Anyone can submit a slashing request with the evidence of Double Sign, which should contain the 2 block headers with the same height and parent block, sealed by the offending validator.

To encourage all users in the network, the slash submitter will get 1000 PRB reward if the evidence is accepted.

In case of any kind of interruption, the validator will go to jail until the next round of delegator election and won't be able to claim any share from the rewards.

4.4 Randao Random Number Generator Contract

As explained in Section 2.1.3, Randao contract has been implemented for later to generate a random number between validators. This method will allow the validators observe the process and create a fair environment for all the participators.

There are two main steps to generate random number with the Randao contract:

Step 1: Collecting valid SHA3(s).
Each main validator must create a cryptographically random number ident_i in its own turn (say i-th block) in the consensus. Using ident_i, the validator first computes the random hash secret s_i = Keccak (Keccak(key,ident_i),ident_i) where key is the private key of the validator and its committed value of hash secret comm_i= Keccak(s_i). The pair value (ident_i,comm_i) along with open value of previously committed value (s_k, where k < i) are sent to Randao contract as a transaction.

Step 2: Calculation of the random number.
Randao contracts stores a global seed value (256-bit) (initially is set to zero). Once a committed random hash value is opened, this seed value is

simply XORed with the opened value. In this context, Randao contract will check if open value (s_k) is valid by running Keccak against s_k and comparing the result with previous committed data. The current s_k will be used to update the global seed value (seed := seed $\oplus$ s_k). If any main validator fails to send a valid s_k value, this will increase the number of block misses for that major validator.

4.5 Governance Contract

Blockchain networks are autonomous platforms that develop themselves with the contribution of the community. On-chain Governance is the system for recommending and implementing changes in cryptocurrency blockchains. In this type of governance, change initiation rules are hard coded into the blockchain protocol. The main validators which are also selected by the community propose possible ideas through code updates and written proposals. All stake holders include all validators, standby validators, normal users vote on whether to accept the proposed change.

With the governance contract, the community members will be able to vote on the proposals to contribute to the development of the blockchain network. The eligible members (which stake enough PRBs) of the community can vote for these proposals. There is also a report option on the governance contracts to report inconvenient usage of the contracts. The following parameters are subject to change by the decision of community:

• Minimum amount of required stake for being a candidate validator (initially is set to 10,000).

• Enabling or disabling application for being a candidate validator.

• The fee for a proposal of a parameter update
(min = 10 PRB, max = 1,000 PRB).

• The revenue percentage for any validators (min = 20, max = 100).

4.4 Rewards per Share

Both the update of validator set, and distribution of rewards are performed for every block. It is possible to stake at any time during the day. During the initialization, the validator pool is set to empty. Reward per share is calculated when staking is received in the validator pool. Let *RPS* be Reward Per Share and *LSRPS* be the Latest Saved RPS which is the validator's current RPS, recorded after a user takes any action (staking, unstaking, claiming). Then,

RPS_new= RPS_old + Incoming Staking Amount / Total Staking Amount.

*PendingRewards_U = (RPS_new - LSRPS) * DepositAmount_U where PendingRewards_U denotes the pending rewards amount of the user U, DepositAmount_U denotes the deposited amount of the user U.*

4.4.1 A working example

Assume that a user A stakes 100 PRB on Monday morning.

1st Day:
RPS_old = 0.
RPS_new = 0.
LSRPS_A = 0.
DepositAmount_A = 100.
PoolTotal = 100.
PendingRewards_A = 0.

2nd Day: 10 PRB as rewards come to the pool on Monday night.
*RPS_new = 0 (RPS_old) + 10 *Rewards / 100 PoolTotal = 0.1.*
*PendingRewards_A = (0.1 (RPS_new) - 0 (LSRPS_A)) * 100 (DepositAmount_A) = 10.*

3rd Day: On Tuesday, B deposits 150 PRB.
LSRPS_B = 0.1 (The current RPS in the pool).
PoolTotal = 250.
20 PRB awards come at night.
RPS_new = 0.1 (RPS_old) + 20 / 250 = 0.18
*PendingRewards_A = (0.18 - 0) * 100 = 18.*
*PendingRewards_B = (0.18 - 0.1 (LSRPS_B)) * 150 = 12.*

4th Day: B collects his/her rewards on Wednesday morning.
TotalRewards_B = PendingRewards_B - 12.
LSRPS_B = 0.18.

5th Day: 30 PRB rewards come Wednesday night.
RPS_new = 0.18 + 30 / 250 = 0.3.
*PendingRewards_A = (0.3 - 0) * 100 = 30.*
*PendingRewards_B = (0.3 - 0.18) * 150 = 18.*

4.5 Future Implementations: Additional Features of Paribu Net

4.5.1 Layer 2 Enhancement: Low-cost Verification through ZKRollup

Paribu Net aims to provide compatibility and support Layer 2 solutions which is a promising technology to improve the scalability of Layer 1 significantly. Optimistic rollups rely on fraud proofs while ZKRollups rely on ZKSNARK [11,30,28]. Since ZKRollups are far more secure than optimistic rollups due to various reasons (finality, data availability, withdrawal time) we aim to support ZKSNARK based solutions on Paribu Net. In a ZKSNARK proof system [13, 15, 20, 25]), there is a prover who wants to convince a verifier that some statement is true without revealing any other information, e.g., the verifier learns that the prover has more than X in his bank account but nothing else (i.e., the actual amount is not disclosed). A ZKSNARK proof allows one to efficiently verify the validity of statements without learning about the inputs. ZKSNARKs are one of the most popular zero-knowledge

proofs due to its practicality where the size proof is succinct which lead to efficient verifications. In particular, the proofs can be verified very quickly (in few milliseconds). Therefore, these mechanisms got a lot of attention due to its in efficiency in large-scale distributed systems and is being used to provide privacy-preserving systems.

4.5.2 Improvement of Node Stability with Erigon

In order to improve the tps, performance in terms of on-chain crawling and faster synchronization for the archive and validator nodes we aim to develop our clients with Erigon which has significant advantages over Geth for supporting consensus upgrades [31].

4.5.3. Gas Sponsorship

Gas sponsorship option has already been supported by different projects (e.g., Ontology [9]), and it allows some other users in the same blockchain network to pay transaction fees. It is also going to be a desired option for Paribu Net where users would be able to delegate others to pay gas fees for their transactions. This feature is going to be useful for enterprise users and cryptocurrency exchanges to regulate their gas payment. We aim to follow the instructions of EIP-4337 for the future implementation of the gas sponsorship option [1].

5. Potential Functionalities on top of Paribu Net

5.1 Data Security

Paribu Net will also provide secure communication and efficient secure data transmission by eliminating the centralized trust of existing conventional systems. Threshold homomorphic encryption systems is an asymmetric encryption protocol that combines two different well-known encryption properties: threshold encryption and homomorphic property [26]. In a (t,n) threshold encryption scheme, the private (decryption) key is split into

shares such that any t-out-of-n partial decryptions can be combined into a complete decryption of a given ciphertext in a single round. Therefore, it also allows protecting the private keys by eliminating the single point of failure. Homomorphic encryption, on the other hand, allows data to be encrypted and outsourced to cloud in such a way that data computations without decryption. This property can be used for businesses and organizations such as financial services, password-based authentication, retail, and healthcare to allow people to use data without disclosing the data in plain form (e.g., analysing medical data without compromising privacy of individuals).

5.2 Secure Wallets and Multi-Chain Bridges through Threshold Signature

One of the most important future plans of Paribu Net is to provide threshold signatures (e.g., threshold ECDSA/BLS/EdDSA) as a crypto library/service for users to be able to implement DApps and bridges for cross chains. Threshold signatures have potential to provide a cheap and effective way to create signatures eliminating single-of-point-of-failure. This protocol relies on the distributed key generation and signing algorithms.

Paribu Net aims to support threshold ECDSA, EdDSA, and BLS signatures which to provide wide functionalities and libraries to its users to allow them to adopt their business models. Hence, these protocols will allow different business and use case adoptions in the future. This threshold signature technology will also be used on the client-side wallet eliminating single point of failure.

5.3 Privacy vs Accountability

Paribu Net always respects privacy of individuals. In this respect, the underlying system aims to provide through smart contracts with DApps:

• the confidentiality of balance where the transferred amount can be both transparent and confidential.

• the freedom to make addresses public or confidential. In this respect, the owner of the address may require the transfers to his/her address to be public or confidential or leave this option to the sender. For example, assume that you have an address as a charity organization, and you want everything to be transparent and visible. Then, you may require all transfers to be sent to this address to be public, or they must all be confidential, or you can leave this option to the sender.

Privacy will be ensured using the advanced cryptographic algorithms/protocols such as Homomorphic Encryption, Threshold Cryptography, and ZKSNARKs. Due to regulations, accountability (through self-sovereign decentralized identity) will also be provided without compromising privacy of honest users.

5.4 Ecosystem Expansion with DApps

The underlying platform will provide community to develop their own projects very quickly such as DeFi, Metaverse, Gaming, Naming services, Supply Chain, Decentralized Storage, and Social Aid Network. These contribute to the growth and expansion of Paribu Net. To promote self-development of a decentralized network, the system will be designed in such a way that anyone who is willing to contribute to the development or expansion of the ecosystem can do so without relying on a single development or community group.

References

[1.] Account abstraction via entry point contract specification. https://eips.ethereum.org/EIPS/eip-4337 .

[2.] ETH PoS process. https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/.

[3.] Ethereum by numbers. https://consensys.net/blog/news/ethereum-by-the-numbers-may-2020/.

[4.] General explanation of PoA consensus protocol. https://tokens-economy.gitbook.io/consensus/chain-based-hybrid-models/ethereum-proof-of-authority.

[5.] Official repos and networks of geth networks. https://github.com/ethereum/go-ethereum.

[6.] Official webpage of ripple cryptocurrency and blockchain project. https://ripple.com/.

[7.] Official webpage of stellar cryptocurrency and blockchain project. https://www.stellar.org/?locale=en.

[8.] Supported transaction types of geth networks. https://github.com/ethereum/go-ethereum/blob/master/core/types/transaction.go.

[9.] Trust redefined: A blockchain for self-sovereign id and data. https://ont.io/, 2017.

[10.] Andreas M Antonopoulos and Gavin Wood. Mastering Ethereum: Building smart contracts and dapps. O'reilly Media, 2018.

[11.] Arbitrum: Scalable, private smart contracts. https://portal.arbitrum.one/, 2021.

[12.] Alireza Beikverdi and JooSeok Song. Trend of centralization in Bitcoin's distributed network. In 2015 IEEE/ACIS 16th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), pages 1-6.IEEE, 2015.

[13.] Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, and Madars Virza. Succinct non-interactive zero knowledge for a Von Neumann Architecture. In Proceedings of the 23rd USENIX Conference on Security Symposium, SEC'14, page 781-796, USA, 2014. USENIX Association.

[14.] Guido Bertoni, Joan Daemen, Michael Peeters, and Gilles Van Assche. Keccak. In Advances in Cryptology - EUROCRYPT 2013, pages 313-314, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[15.] Benedikt Bunz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. Bulletproofs: Short proofs for confidential transactions and more. In 2018 IEEE Symposium on Security and Privacy (SP), pages 315-334, 2018.

[16.] Dan Boneh, Joseph Bonneau, Benedikt Bunz, and Ben Fisch. Verifiable delay functions. In Advances in Cryptology - CRYPTO 2018, pages 757-788, Cham, 2018. Springer International Publishing.

[17.] Dan Boneh, Sergey Gorbunov, Hoeteck Wee, and Zhenfei Zhang. BLS Signature Scheme. (draft-boneh-bls-signature-00), February 2019.

[18.] Chris Dannen. Introducing Ethereum and solidity, volume 318. Springer, 2017.

[19.] Stefano De Angelis, Leonardo Aniello, Roberto Baldoni, Federico Lombardi, Andrea Margheri, and Vladimiro Sassone. PBFT vs Proof-of-Authority: Applying the cap theorem to permissioned blockchain. 2018.

[20.] Jens Groth. On the size of pairing-based non-interactive arguments. In Marc Fischlin and Jean-Seebastien Coron, editors, Advances in Cryptology - EUROCRYPT 2016, pages 305-326, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.

[21.] Don Johnson, Alfred Menezes, and Scott Vanstone. The Elliptic Curve Digital Signature Algorithm (ECDSA). International Journal of Information Security, 1(1):36-63, August 2001.

[22.] Simon Josefsson and Ilari Liusvaara. Edwards-Curve Digital Signature Algorithm (EdDSA). (8032), January 2017.

[23.] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. http://www.bitcoin.org/bitcoin.pdf, 2009.

[24.] U.S. Department of Commerce, National Institute of Standards, and Technology. Secure Hash Standard - SHS: Federal Information Processing Standards Publication 180-4. CreateSpace Independent Publishing Platform, North Charleston, SC, USA, 2012.

[25.] B. Parno, J. Howell, C. Gentry, and M. Raykova. Pinocchio: Nearly practical verifiable computation. In 2013 IEEE Symposium on Security and Privacy, pages 238-252, 2013.

[26.] Berry Schoenmakers. Threshold Homomorphic Cryptosystems, pages 1293-1294. Springer US, Boston, MA, 2011.

[27.] Adrian Segall. Distributed network protocols. IEEE transactions on Information Theory, 29(1):23-35, 1983.

[28.] Starkware. Starkware. https://starkware.co/, 2021.

[29.] Gavin Wood et al. Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper, 151(2014):1-32, 2014.

[30.] ZKSync. ZKSync-rely on math, not validators. https://zksync.io/, 2021.

[31.] Erigon Community. Erigon - blockdaemon: An ethereum client on the efficiency frontier. https://github.com/ledgerwatch/erigon, 2022.

PARiBU NET

Whitepaper 1.0.0

02 February 2022