PAREX

SMART CHAIN

Whitepaper V.1.0

Contents

1/ The Vision for Web3 Business

Web3 promises to be a revolutionary technology and a decentralized approach to next-generation application development. However, the vision for Web3 businesses is far broader than just a set of tools and technologies. Just like the advent of the Internet in the late 1990s revolutionized how people around the world communicate and interact with each other, new online models emerged at that time that completely displaced existing businesses.

2/ Introduction

Since the publication of the Bitcoin whitepaper in 2008, the concept of blockchain has spread across the world. While decentralized money and applications are becoming well-publicized ideas, design limitations have challenged the core aspiration of Bitcoin. The original Bitcoin blockchain was designed as a peer-to-peer payment system that allows people to transfer value without intermediaries like banks or payment processors. However, as Bitcoin gained popularity, its performance bottleneck became evident due to its limited throughput of ~7 transactions per second (TPS), and its cost as a payment system became prohibitively expensive.

In 2014, Buterin et. al. proposed a new blockchain infrastructure called Ethereum, which enabled developers to create various kinds of blockchain applications using “smart contracts.” However, Ethereum didn’t solve the scalability problem and, with its ~15 TPS, failed to support high-throughput applications such as gaming or decentralized exchanges.

Given Ethereum and Bitcoin’s performance limitations, many blockchain projects proposed various solutions that attempt to increase transaction throughput. Various blockchains proposed to replace Proof-of-Work (PoW) consensus with Proof-of-Stake (PoS) consensus. Other blockchains like EOS use Delegated Proof of Stake (DPoS), where block proposers are elected by voting rather than by an on-chain algorithmic process

We introduce Parex Smart Chain, the next generation blockchain that is fully scalable,provably secure, and energy efficient. Parex addresses the problems of existing blockchains by combining the best research results and engineering practice in an optimally tuned system. Specifically, Parex makes breakthroughs in following aspects:

Fully Scalable: Parex shards not only the network communication and transaction validation, but also shards the blockchain state. This makes Parex a fully scalable blockchain.

Secure Sharding: Parex's sharding process is provably secure thanks to the distributed randomness generation (DRG) process which is unpredictable, unbiaseable, verifiable and scalable. Parex also reshards the network in a non-interruptive manner to prevent against slowly adaptive byzantine adversaries.

Efficient and Fast Consensus: Unlike other sharding-based blockchains which require PoW to select validators, Parex is based on PoS and thus energy efficient. Consensus is reached with a linearly scalable BFT algorithm that's 100 times faster than PBFT.

Adaptive-Thresholded PoS: The threshold of stakes required for a node to join the network is adjusted based on the volume of total staking in a way that malicious stakers cannot concentrate their power in a single shard. Moreover, the threshold is low enough so that small stakers can still participate in the network and earn rewards.

Consistent Cross-Shard Transactions: Parex supports cross-shard transactions with shards directly communicating with each other. An atomic locking mechanism is used to ensure the consistency of cross-shard transactions.

By innovating on both the protocol and network layers, Parex provides the world with a scalable and secure blockchain system that is able to support the emerging decentralized economy. Parex will enable applications which were not previously feasible on blockchain, including high-volume decentralized exchanges, payment systems, and Internet-of-Things transactions. Parex strives to scale trust for thousands of people and create a radically fair economy.

3/ Consensus Mechanism

The consensus protocol is a key component of any blockchain. It determines how securely and quickly blockchain validators reach consensus on the next block. The first blockchain consensus 1 protocol which powers Bitcoin is Proof-of-Work (PoW) consensus. PoW is a process whereby miners race to find the solution to a cryptographic puzzle the winner gets the right to propose the next block and earns some token rewards. PoW's security assumption is that more than 50% of the hashing power is controlled by honest nodes. With such an assumption, the rule for consensus is that the longest chain will be the canonical one, and thus PoW consensus is also called chain-based consensus.

Another type of consensus protocol, one which has been researched for more than two decades in academia, is called PBFT (Practical Byzantine Fault Tolerance). In PBFT, one node is elected as the "leader," while the rest of the nodes are "validators." Each round of PBFT consensus involves two major phases: the prepare phase and the commit phase. In the prepare phase, the leader broadcasts its proposal to all of the validators, who in turn broadcast their votes on the proposal to everyone else. The reason for the rebroadcasting to all validators is that the votes of each validator need to be counted by all other validators. The prepare phase finishes when more than $2f + 1$ consistent votes are seen, where f is the number of malicious validators, and the total number of validators plus the leader is $3f + 1$. The commit phase involves a similar vote counting process, and consensus is reached when 2f + 1 consistent votes are seen. Due to the rebroadcasting of votes among validators, PBFT has $O(N^2)$ communication complexity, which is 2 not scalable for a blockchain system with hundreds or thousands of nodes.

As an improvement on PBFT, Parex's consensus protocol is linearly scalable in terms of communication complexity, and thus we call it Fast Byzantine Fault Tolerance (FBFT). In FBFT, instead of asking all validators to broadcast their votes, the leader runs a multi-signature signing process to collect the validators' votes in a O(1)-sized multi-signature and then broadcast it. So instead of receiving O(N) signatures, each validator receives only one multi-signature, thus reducing the communication complexity from $O(N^2)$ to O(N).

The idea of using O(1)-sized multi-signature is inspired by ByzCoin's BFT which uses the Schnorr signature scheme for constant-sized multi-signature aggregation and forms a multicast tree among validators to facilitate the message delivery. However, a Schnorr multi-signature requires a secret commitment round, which leads to a total of two round-trips for a single multi-signature. Parex improves upon that by using BLS (Boneh–Lynn–Shacham) multi-signature, which only requires one round-trip. Therefore, FBFT is at least 50% faster than ByzCoin's BFT. The fountain code broadcasting technique also avoids a security issue in ByzCoin's original tree-based multicasting design.

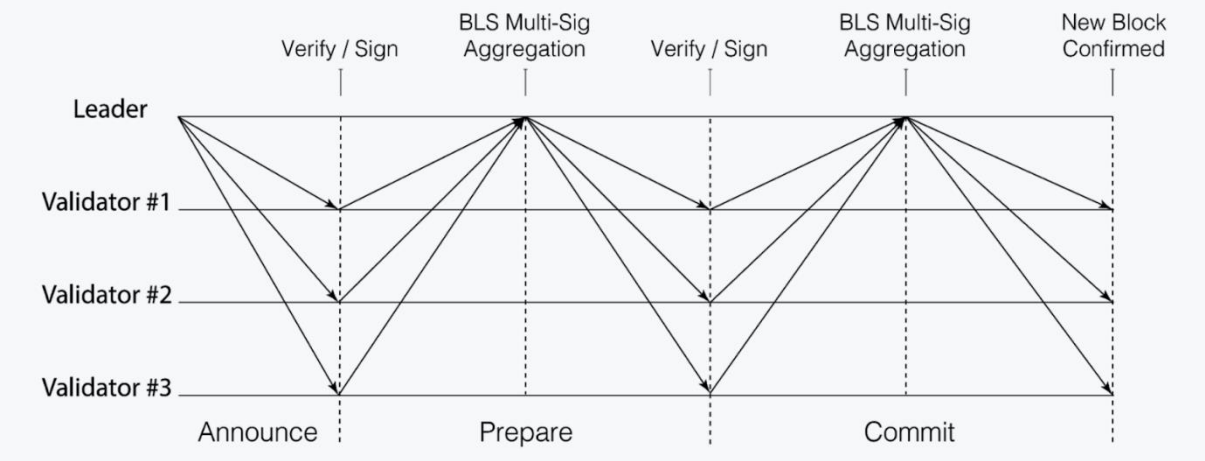


Figure: Network communication during a single round of consensus.

Specifically, Parex's FBFT consensus involves the following steps:

1. The leader constructs the new block and broadcasts the block header to all validators. Meanwhile, the leader broadcasts the content of the block with erasure coding. This is called the "announce" phase.

2. The validators check the validity of the block header, sign the block header with a BLS signature, and send the signature back to the leader.

3. The leader waits for at least $2f + 1$ valid signatures from validators (including the leader itself) and aggregates them into a BLS multi-signature. Then the leader broadcasts the aggregated multi-signature along with a bitmap indicating which validators have signed. Together with Step 2, this concludes the "prepare" phase of PBFT.

4. The validators check that the multi-signature has at least $2f + 1$ signers, verify the transactions in the block content broadcasted from the leader in Step 1, sign the received message from Step 3, and send it back to the leader.

5. The leader waits for at least $2f + 1$ valid signatures (can be different signers from Step 3) from Step 4, aggregates them together into a BLS multi-signature, and creates a bitmap logging all the signers. Finally, the leader commits the new block with all the multi-signatures and bitmaps attached, and broadcasts the new block for all validators to commit. Together with Step 4, this concludes the "commit" phase of PBFT. The validators of Parex consensus are elected based on Proof-of-Stake. Therefore, the actual protocol differs slightly from the one described above in a sense that a validator with more voting shares has more votes than others, rather than one-signature-one-vote. So instead of waiting for at least $2f + 1$ signatures from validators, the leader waits for signatures from the validators who collectively possess at least 2f + 1 voting shares.

4/ Sharding

Blockchain sharding as a scalability solution has gained lots of attention since late 2017. Various sharding solutions have been proposed both in industry and academia.

In industry, Zilliqa was the first sharding-based public blockchain that claimed a throughput of 2,800 TPS. Zilliqa uses PoW as identity registration process. Zilliqa's network contains a single directory-service committee and multiple shard committee, each containing hundreds of nodes. Transactions are assigned to different shards and processed separately. The resulting blocks from all shards are collected and merged at the directory-service committee. Zilliqa is not a state sharding solution because each node has to hold the entire blockchain state to be able to process transactions.

In academia, publications like Omniledger and RapidChain have proposed solutions that feature state sharding where each shard holds a subset of the blockchain state. Omniledger employs a multi-party computation scheme called RandHound to generate a secure random number, which is used to randomly assign nodes into shards. Omniledger assumes a slowly adaptive corruption model where attackers can corrupt a growing portion of the nodes in a shard over time. Under such security model, a single shard can be corrupted eventually. Omniledger prevents the corruption of shards by reshuffling all nodes in the shards at a fixed time interval called epoch. RapidChain builds on top of Omniledger and proposes the use of the Bounded Cuckoo Rule to reshuffle nodes without interruptions.

Parex draws inspiration from these three previous solutions and designs a PoS-based full sharding scheme that's linearly scalable and provably secure. Parex contains a beacon chain and multiple shard chains. The beacon chain serves as the randomness beacon and identity register, while the shard chains store separate blockchain states and process transactions concurrently. Parex proposes an efficient algorithm for randomness generation by combining Verifiable Random Function (VRF) and Verifiable Delay Function (VDF). Parex also incorporates PoS in the sharding process which shifts the security consideration of a shard from the minimum number of nodes to the minimum number of voting shares.

Parex will be able to process anywhere from 10,000 to 20,000 transactions per second with sharding.

5/ Epochs

In Parex, the consensus and sharding process is orchestrated by the concept of epochs. An epoch is a predetermined time interval during which the sharding structure is fixed and each shard continuously runs consensus with the same set of validators. At the beginning of each epoch, a random number will be generated using the DRG protocol and the sharding structure will be determined based on that randomness. Validators who want to validate transactions in epoch e need to stake their tokens during epoch $e-1$. The cutoff time for staking is before the randomness preimage pRnd is committed into the blockchain.

6/ Adaptive-Thresholded PoS

The price of a voting share is set algorithmically so that it's small enough that malicious stakers can not concentrate their voting power in a single shard. Specifically, we set the price of a voting share to be P_{vote} tokens:

$$P_{vote} = \frac{TS_{e-1}}{NumShard * \lambda}$$

Here λ is a security parameter, NumShard is the number of shards and TS_{e-1} is the total amount $e-1$ of tokens staked during epoch $e-1$.

Now we prove that when λ > 600, the chance of a single shard having more than malicious $\frac{1}{3}$ voting shares is negligible.

Given the definition of P_{vote}, the total number of voting shares will be $N = \frac{TS_{e-1}}{P_{vote}} = NumShard * \lambda$ Given a trustable randomness source and the sharding process based on the randomness, the probability distribution of the number of malicious voting shares in each shard can be modeled as a hypergeometric distribution (i.e. random sampling without replacement):

$$P(X = k) = \frac{\binom{K}{k}\binom{N-K}{n-k}}{\binom{N}{n}}$$

Here N is the total number of voting shares, $K = \frac{N}{4}$ is the maximum number of malicious voting shares, $n = \frac{N}{NumShard}$ is the number of voting shares in each shard, and is the number of malicious voting shares in a shard. The actual failure rate of a shard $P(X \leq k)$ follows cumulative hypergeometric distribution $CDF_{hg}(N, K, n, k)$ which, when N is large, degrades to binomial distribution (i.e. random sampling with replacement):

$$P(X \leq k) = \sum_{i=0}^{k} \binom{n}{i} p^i (1-p)^{n-i}$$

We can show that when n is large enough, the probability that a shard contains more than 3 1 tokens held by malicious entities is negligible. In fact, when n = 600 , the probability that a shard contains less than malicious voting shares is , which translates to a shard 3 1 $P(X \leq 2000)$ = 0.999997 failure (i.e. consensus cannot be reached) rate of “once in around 1000 years” (given an epoch interval of 24 hours). Therefore, we will set λ = 600 to guarantee the high security of our shards. (Intuitively, λ governs minimum number of voting shares a single shard should contain. This is functionally similar to the minimum number of nodes in a shard as described in other PoW-based sharding solutions)

This approach is resistant to the fluctuation of the number of validators. We are not setting a lower limit on number of validators in each shard as in other solutions like Zilliqa. Instead, we adopt an adaptive PoS-based model to ensure that the malicious people can never occupy more than $\frac{1}{3}$ of the voting shares in a single shard, thus making it secure.

7/ Native Coin

Parex (PRX) is the native coin of Parex Smart Chain. Both cross- and intra-chain transactions consume a certain amount of Parex. Parex is also used in security deposits for the cross-chain verification nodes.

8/ Background for Application of Parex Smart Chain

8.1/ Payment Method

More and more businesses accept digital assets, like Bitcoin, as a means of payment. In the future, there will be more applications in which a variety of digital currencies are used for payments. Currently, there are many payment methods such as VISA, Paypal and Alipay, each with their own payment procedures and settlement processes. Parex Exchange is a distributed multi-currency platform. Any business or user can install the Parex wallet to implement multi-currency payments and settlements without having to install multiple digital currency wallets.

8.2/ PEP20 Tokens

PEP20 (Parex Smart Chain Evolution Proposal) token is a type of virtual asset that is based on the Parex Blockchain.

PEP20 tokens are virtual assets running on the Parex blockchain; they have value and users can send and receive them. People can create these tokens via smart contracts on the Parex network.

8.3/ Social & Fan Tokens

Social & Fan tokens are digital cryptocurrencies offered by various sports clubs and associations that help them monetize and engage with their fan bases in different ways. Fans benefit from supporting their favorite club or team in a unique way, and receive exciting benefits by holding their club's tokens. These clubs or organizations can create PEP20 tokens for their own goals.

8.4/ Staking

There will be some advantages and gains for stakers. Parex is constantly organizing new rates and many campaigns. Staking can be done not only for the main coin, but also for PEP20 coins using smart contracts.

8.5/ Game Industry & Metaverse

PRX and PEP20 tokens can be used in many games by determining the value with the tokens used in the game industry and metaverse with the agreements made. The best example of this is the swap method.

8.6/ Advert & Survey

PEP10 is a native token on the Parex blockchain (unlike the PEP20 token) that is a standard of basic token production and does not require the Parex Virtual Machine (PVM). You can access PEP10 through an API. The transaction fees of the PEP10 token are 100 times lower than the ones of the PEP10 token. Advertising and survey transactions can be done by creating a PEP10 contracts.

8.7/ Internet of Things (IOT)

The current Internet of Things system depends on a centralized network management architecture where all devices are connected through a cloud server. But in a decentralized Internet of Things system, Blockchain can create a basic framework to facilitate the transaction and cooperation of devices. Each device on the network functions as an independent, micro business entity.

8.8/ AI Architectures and Algorithms

-Symbolic Learning and Reasoning

This work involves integrating multiple AI tools, such as the probabilistic logic networks logic engine, the PEPES automated program learning engine, the OpenCog pattern miner, and the ECAN attention allocation system, into a common framework based on OpenCog's unified rule engine.

Conceptually, the key theme is leveraging reflective meta-learning and cognitive synergy (win–win interoperation between different cognitive algorithms) to achieve higher levels of generalization and abstraction in machine learning/reasoning.

-Scalable, General Probabilistic Logic

Modern computing resources,data sources, and theoretical advances make it feasible to integrate logical inference with probabilistic and statistical inference in an intricate manner.

The ability to relate problems (theorems) to their solutions (proofs) in a transparent manner is particularly suited to complex tasks such as bringing heterogeneous processes to inter-operate with each other, providing a link between machine understanding and human understanding, and enabling deep levels of introspection and meta-learning.

The "generalization" part of artificial general intelligence is something that logical systems are especially good at, more so than deep neural networks or other forms of AI that originate in pattern-analysis and "curve-fitting."

- Integrative Genomics as a Case Study for Integrative AI

As biology becomes an information science and information science becomes dominated by machine learning and other AI methods, it stands to reason that biology is becoming dominated by AI. To grapple with the systemic nature of disease and aging, it is necessary to do simulation modeling, data analysis, and machine reasoning regarding the multiple body subsystems across numerous datasets.

Concurrency in OpenCog can happen on a logical level, as when components work on the same object, or on a semantic level, as when two components work on the same knowledge-base element (for example, a concept).

Data integrity policies, in this case, need to manage a configurable tradeoff between integrity and performance. In other words, data integrity policies need to balance—on the one hand—ensuring that each component see the changes the other makes to a concept and—on the other hand—allowing each component to change concept properties without delay.

Determining the value of a concept property concurrently changed by two or more components is not trivial. This operation (referred to as "merging" in OpenCog) may require complex procedures with side effects (chained changes in other elements of the knowledge base) and can differ according to the type of concept involved.

9/ Conclusion

In this paper, we put forth the concept of a future "bank". The term "bank" is an analogy used to give readers a more intuitive understanding of the concept. Abstracting blockchain technology, from the concept of Bitcoin into a neutral technology, greatly improved the global popularization and application of blockchain, however it still faces huge obstacles. It's risky and expensive for traditional banks to solve existing business problems by using blockchains. Decision makers are unlikely and unwilling to take such a big risk due to investor return expectations, and for just one bank to change is not enough. The financial framework based on digital currency is like traditional banking at the business level but is different in its nature and organization. This is similar to what occured at the inception of ecommerce, which did not sprout from traditional industries, but generated new commercial modalities that changed the traditional industries. As the proportion of digital currency in the economy increases, new financial industries based digital currency will flourish. Of course, given time, traditional banks will join the digital currency economy in their own ways and a financial ecosystem integrating traditional assets with digital assets will gradually be developed.

Parex aims to design a new decentralized financial infrastructure, that allows the exchange of value among different blockchain networks. Based on this new model, intermediaries will develop their own financial services and build a distributed super financial market via Parex. We believe that a flexible, decentralized, value exchange system is the future of the financial infrastructure, and will help to promote financial inclusion and standardize future financial transactions.

10/ DAO:

Decentralized autonomous organization in Parex Chain

Decentralized autonomous organizations are typified by the use of blockchain technology to provide a secure digital ledger to track digital interactions across the internet, hardened against forgery by trusted timestamping and dissemination of a distributed database. This approach eliminates the need to involve a mutually acceptable trusted third party in any decentralized digital interaction or cryptocurrency transaction. The costs of a blockchain-enabled transaction and of the associated data reporting may be substantially offset by the elimination of both the trusted third party and of the need for repetitive recording of contract exchanges in different records. For example, the blockchain data could, in principle and if regulatory structures permit it, replace public documents such as deeds and titles. In theory, a blockchain approach allows multiple cloud computing users to enter a loosely coupled peer-to-peer smart contract collaboration.

The rules of the DAO are established by a core team of community members through the use of smart contracts. These smart contracts lay out the foundational framework by which the DAO is to operate. They are highly visible, verifiable, and publicly auditable so any potential member can fully understand how the protocol is to function at every step.

Once these rules are formally written onto the blockchain, the next step is around funding: the DAO needs to figure out how to receive funding and how to bestow governance.
This is typically achieved through token issuance, by which the protocol sells tokens to raise funds and fill the DAO treasury.

In return for their fiat, token holders are given certain voting rights, usually proportional to their holdings. Once funding is completed, the DAO is ready for deployment.

At this point, once the code is pushed into production, it can no longer be changed by any other means other than a consensus reached through member voting. That is, no special authority can modify the rules of the DAO; it is entirely up to the community of token holders to decide.

Every transaction on the Parex Chain undergoes community approval. Most importantly, the commission fees from every transaction made on the Parex chain are given back to the community/burn.

11/ Parex Chain Utility Coin (PRX)

Parex is a decentralized exchange. It also has a token that can only exist through the mining production mechanism. The production network is processed with the PEP-2 protocol. It can also build bridges with many networks thanks to Proof of Interoperability.

11.1/ Pos&Node

The difference between POS and Node and crypto mining versus GPU and SSD mining. First, let's examine what these terms are:

* POS: Proof Of Stake: The reward given to people who hold certain amounts of the relevant crypto money is crypto money. (max. per year 15%)

* Node: Computer nodes are what make it possible to use Blockchain as a peer-to-peer (P2P) decentralized digital network network. The more Nodes there are, the more reliable these networks will be. Cryptocurrency rewards can be earned by keeping a node.

* GPU mining: Crypto mining with high-cost graphics cards

* SSD mining: Crypto mining obtained by performing heavy operations on SSD.

So what is Pos & Node?

As the name suggests, it is a system consisting of a combination of Proof Of Stake and Node. In this system, both POS and Node You are combining your rewards. Thus, a higher rate of reward than other crypto production mechanisms you can receive. The ParexChain blockchain blends proof of stake and node systems, thanks to a self-developed generation algorithm. has developed a brand new, simple and plain crypto production mechanism that appeals to every user base.

11.2/ Private Cloud

Parex production is done from the "My Cloud" menu on the Parex Market mobile application. In order to create a Parex package, you must have enough PRX in your wallet. Tracker installation is required in order to produce parex with the Private Cloud option.

After performing the Traker installation, production packages can be created from the “My Clouds” menus.

Parex Packages can be made with 1,000 PRXs.

Creating a Private Cloud PRX Package:

It can be done with 1/1 -> 1.000 PRX. (Fee required for this transaction is 10 PRX)

Required amount of PRX “Parex Wallet” must be in your wallet.(1.010 PRX)

Operations are continued through the Parex Mobile App / Dashboard / My Clouds menu.

Package Type;

At this stage, we continue our transactions by selecting the "Private" section.

Package Rate;

1/1 Package can be selected from this section.

By clicking the "BUY" button, the Parex package is created.

PRX packages are staked for 365 days. There is no cancellation. The PRXs used for the package are sent to the Burn (CX00000000000000000000000000000000) wallet and banned from circulation. At the end of 365 days, Parex packages are canceled and the coins used are not refundable because they are burned.

After the package is created, you can see the package you have created from the "LIST" menu. Each parex package has its own unique CloudCode (PXCM….). Packages created with this code are connected to the trackers.

Tracker connection with Parex package;

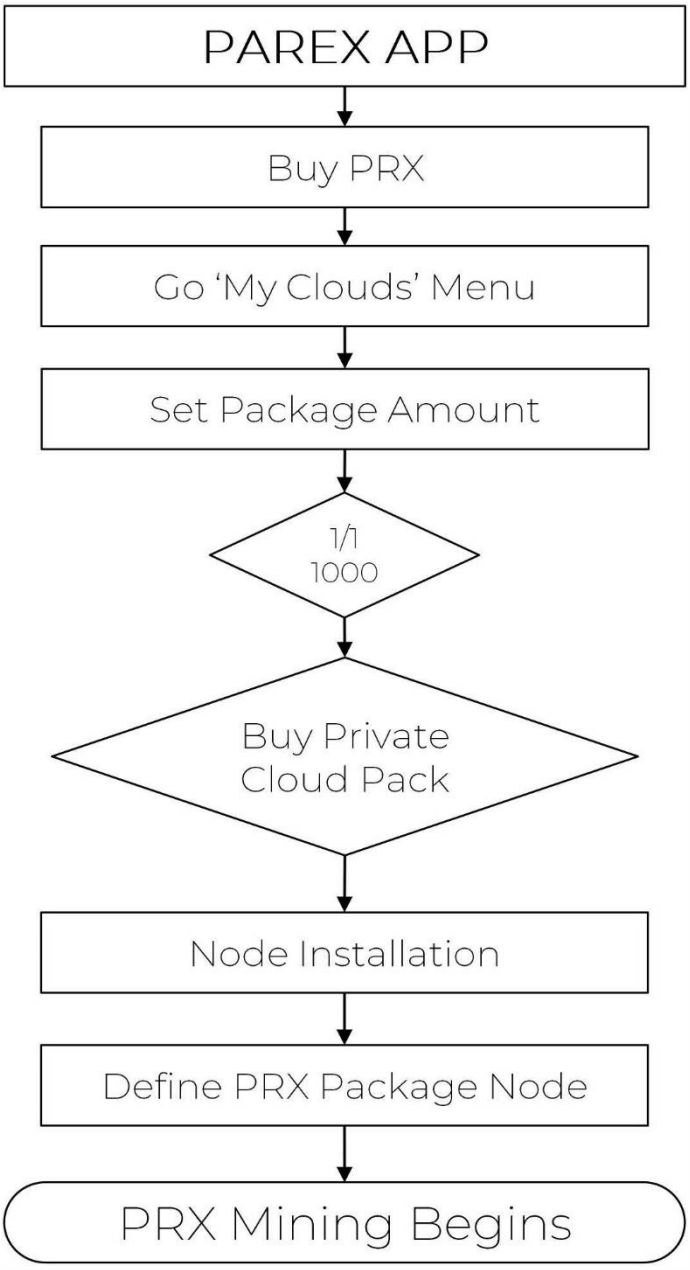
After installing the Tracker and running the Parex Container, a Master Tracker connection must be made first. Since the trackers receive the data from the Master trackers, production cannot be made if this process is not done. The connection code is as follows.

http://{DockerHostIP}:2020/setJoinPool/{poolapikey}

After the repository connection is made, CloudCode (PXCM….) is defined. The identification code is as follows.

http://{DockerHostIP}:2020/setCloudTracker/{cloudcode}

INCOME TRACKING



Please review the production algorithm table for Parex production rates.

Each tracker is connected and pays a "service fee" to Master Tracker, from which it receives data service. This price is determined by the Master tracker itself. Fee at the determined rate is covered from the produced PRX. You can find the "poolapikey" and "service fee" rates from the master tracker list. https://parexscan.io/?#/dashboards/mastertracker

Private Cloud packages that are offline for 24 hours fall into the “Waiting Cloud Trackers” table and are treated as Public Cloud.

11.3/ Public Cloud

Parex production is done from the "My Clouds" menu on the Parex Market mobile application. In order to create a Parex package, you must have enough PRX in your wallet. Tracker installation is not required to produce parex with the Public Cloud option.

Public Cloud; Users who apply to Master Trackers in order to produce. After creating a package as a Public Cloud, any MasterTracker repository is expected to accept the application.

PRX Packages can be made with 1,000 PRXs. Creating a Public Cloud PRX Package:

It can be done with 1/1 -> 1.000 PRX. (Fee required for this transaction is 10 PRX)

The required amount of PRX “Parex Wallet” should be in your wallet (1,010 PRX)

Operations are continued through the Parex Mobile App / Dashboard / My Clouds menu.

Package Type;

At this stage, we continue our transactions by selecting the "Public" section. Package Rate;

1/1 Package can be selected from this section.

By clicking the "BUY" button, the Parex package is created.

PRX packages are staked for 365 days. There is no cancellation. The PRXs used for the package are sent to the Burn (CX0000000000000000000000000000000000) wallet and banned from circulation. At the end of 365 days, Parex packages are canceled and the coins used are not refundable because they are burned.

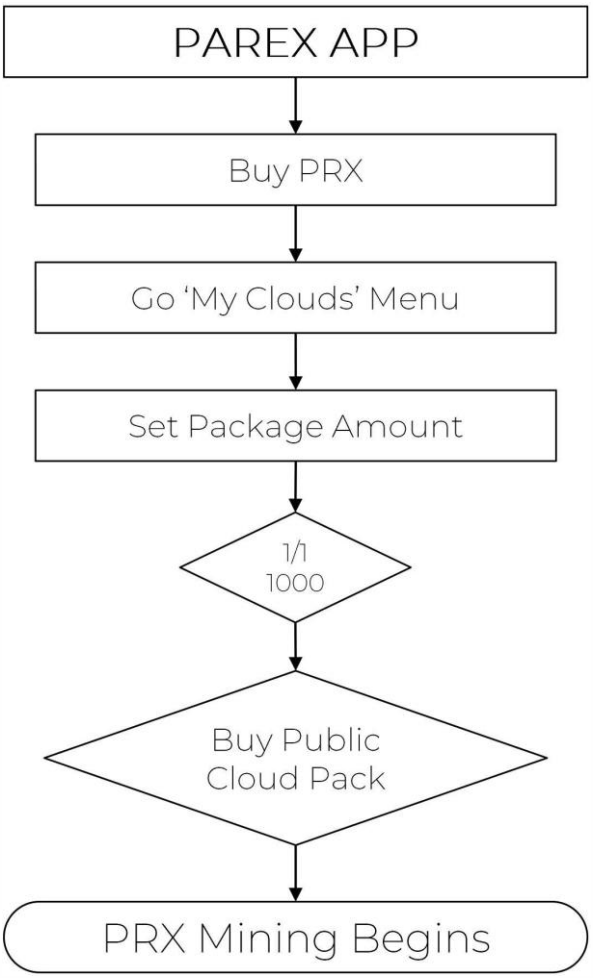
After the package is created, you can see the package you have created from the "LIST" menu. Each parex package has its own unique CloudCode (PXCM….). Packages created with this code are connected to the trackers.

As soon as the Public Cloud account is created, it falls into the “Waiting Cloud Tracker” list. https://parexscan.io/?#/dashboards/dexcommunity

Production will begin when any Master Tracker accepts the application and completes the installation process.

The "Percent %" part in the application list starts with 5% and increases every 1 hour until it reaches 25%. After 25% it starts all over again at 5%.

INCOME TRACKING



Please review the production algorithm table for Parex production rates.

Each tracker pays a "service fee" to Master Tracker, which it is connected to and receives data service from. This price is determined by the Master tracker itself. Fee at the determined rate is covered from the produced PRX. You can find the "poolapikey" and "service fee" rates from the master tracker list. https://parexscan.io/?#/dashboards/mastertracker

Public Cloud packages that are offline for 2 hours fall back into the “Waiting Cloud Trackers” table.

11.4/ Partner Cloud

Parex production is done from the "My Clouds" menu on the Parex Market mobile application. In order to create a Parex package, you must have enough PRX in your wallet. Tracker installation is not required to produce parex with the Partner Cloud option.

Partner Cloud; They are user groups that apply to Master Trackers in order to produce. Partner Cloud packages are a common platform created by users with different PRX numbers. Any MasterTracker pool is expected to accept the application after reaching 1,000 PRX.

Creating a Partner Cloud PRX Package:

Partner Cloud offers different options.

It can be done with 1/2 -> 500 PRX. (Fee required for this transaction is 5 PRX) It can be done with 1/4 -> 250 PRX. (The Fee required for this transaction is 2.5 PRX)

It can be done with 1/10 -> 100 PRX. (Fee required for this transaction is 1 PRX) It can be done with 1/20 -> 50 PRX. (The Fee required for this transaction is 0.5 PRX)

Depending on the feature of the selected package, the required amount of PRX “Parex Wallet” should be in your wallet.

Operations are continued through the Parex Mobile App / Dashboard / My Clouds menu.

Package Type;

At this stage, we continue our transactions by selecting the "Partner" section. Package Rate;

From this section, you can choose any package from 1/2 - 1/4 - 1/10, 1/20 options.

By clicking the "BUY" button, you are included in the Partner Cloud package.

PRX packages are staked for 365 days. There is no cancellation. The PRXs used for the package are sent to the Burn (CX0000000000000000000000000000000000) wallet and banned from circulation. At the end of 365 days, Parex packages are canceled and the coins used are not refundable because they are burned.

After the package is created, you can see the package you have created from the "LIST" menu. Each parex package has its own unique CloudCode (PXCM….). Packages created with this code are connected to the trackers.

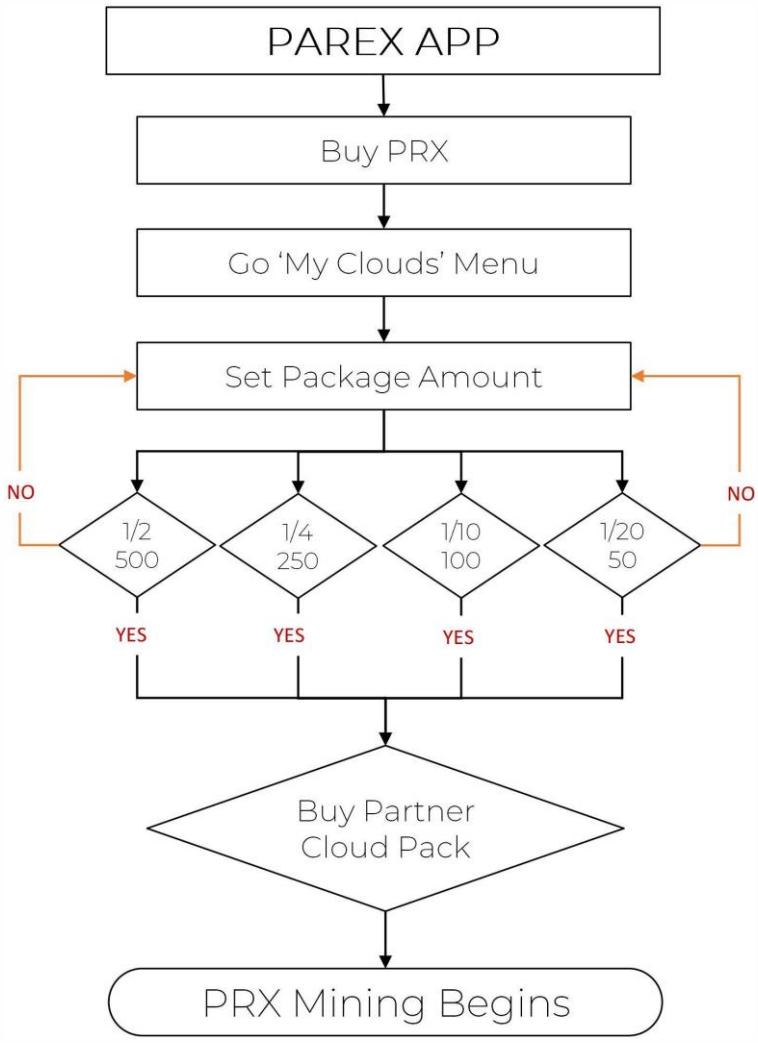
As soon as the Partner Cloud package reaches 1.010 PRX, it falls into the “Waiting Cloud Tracker” list. https://parexscan.io/#/dashboards/ dexcommunity

Production will begin when any Master Tracker accepts the application and completes the installation process.

The "Percent %" part in the application list starts with 5% and increases every 1 hour until it reaches 25%. After 25% it starts all over again at 5%.

*Package start times for packages created with Partner Cloud start when 1000 PRX accumulates and Package occurs and falls on the Waiting Cloud list.

INCOME TRACKING



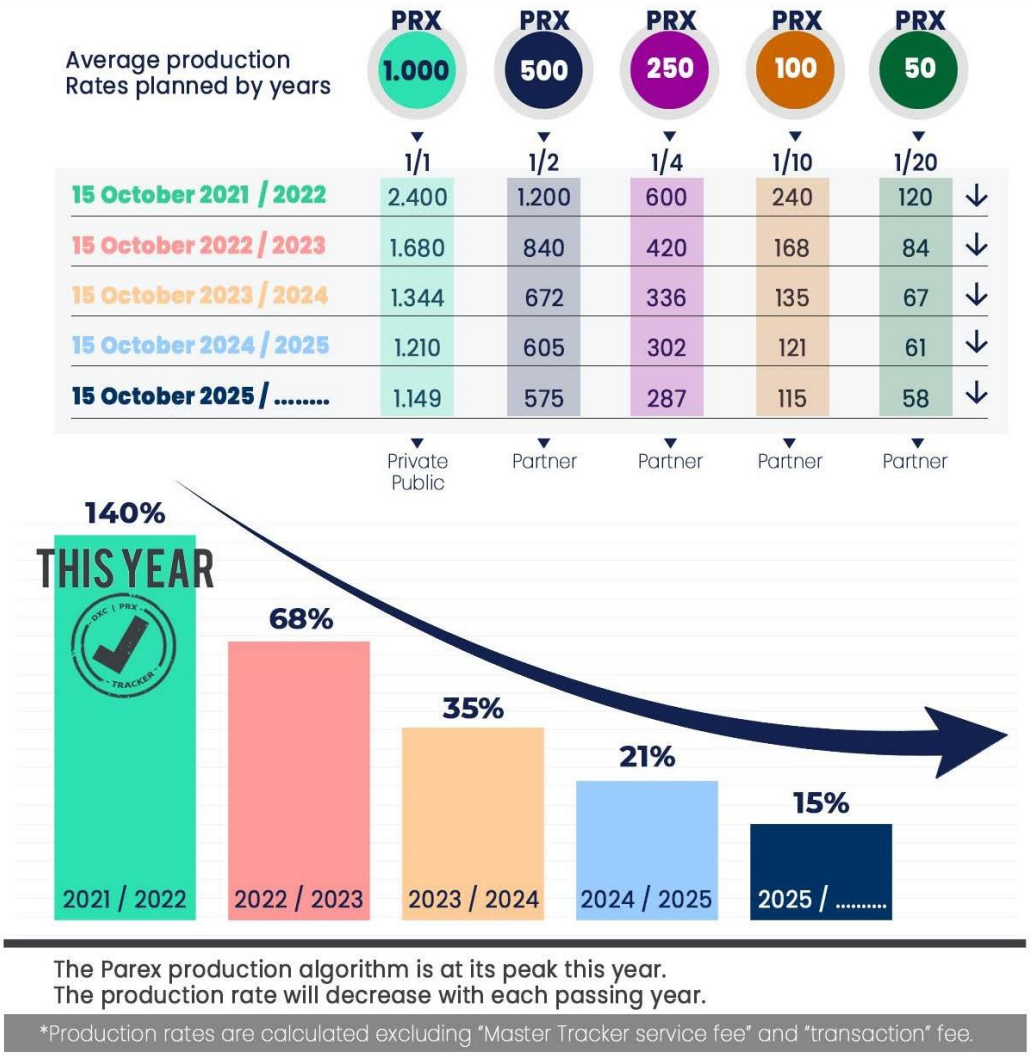
Partner Cloud revenues are allocated to each included package in proportion to the package amount.

Please review the production algorithm table for Parex production rates.

Each tracker pays a "service fee" to Master Tracker, which it is connected to and receives data service from. This price is determined by the Master tracker itself. Fee at the determined rate is covered from the produced PRX. You can find the "poolapikey" and "service fee" rates from the master tracker list. https://parexscan.io/#/dashboards/ mastertracker

* Partner Cloud packages that are offline for 2 hours fall back into the “Waiting Cloud Trackers” table.

11.5/ Parex Annual Production Changes

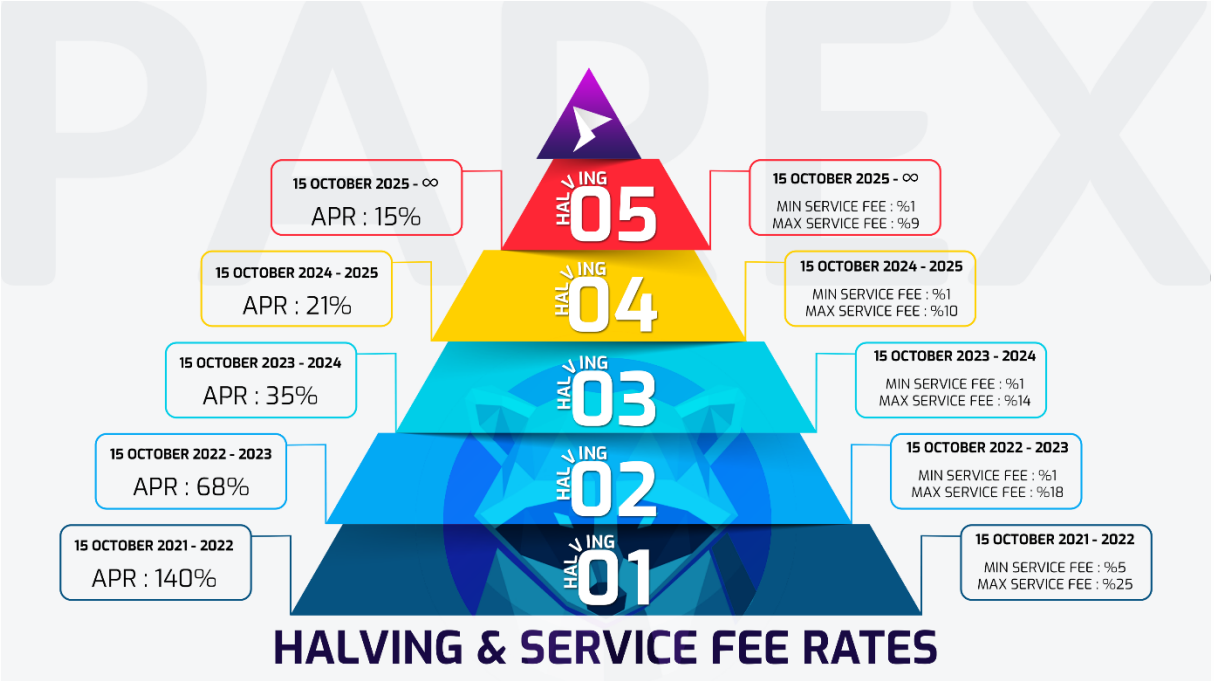


Parex Production Rates are indexed with the annual halving mechanism.

Halving & Service Fee Rates:

Parex has introduced another improvement for its miners.

Parex is known for its constantly evolving structure and unique mining algorithm. As it is known, Parex mining is based on 2 principles. Burning PRX and supporting Blockchain decentralization. So keep NODE. Retained Nodes must connect to a master tracker. Master trackers receive a service fee at certain rates in return for the service they provide. Service charges are automatically covered from the miner's production.

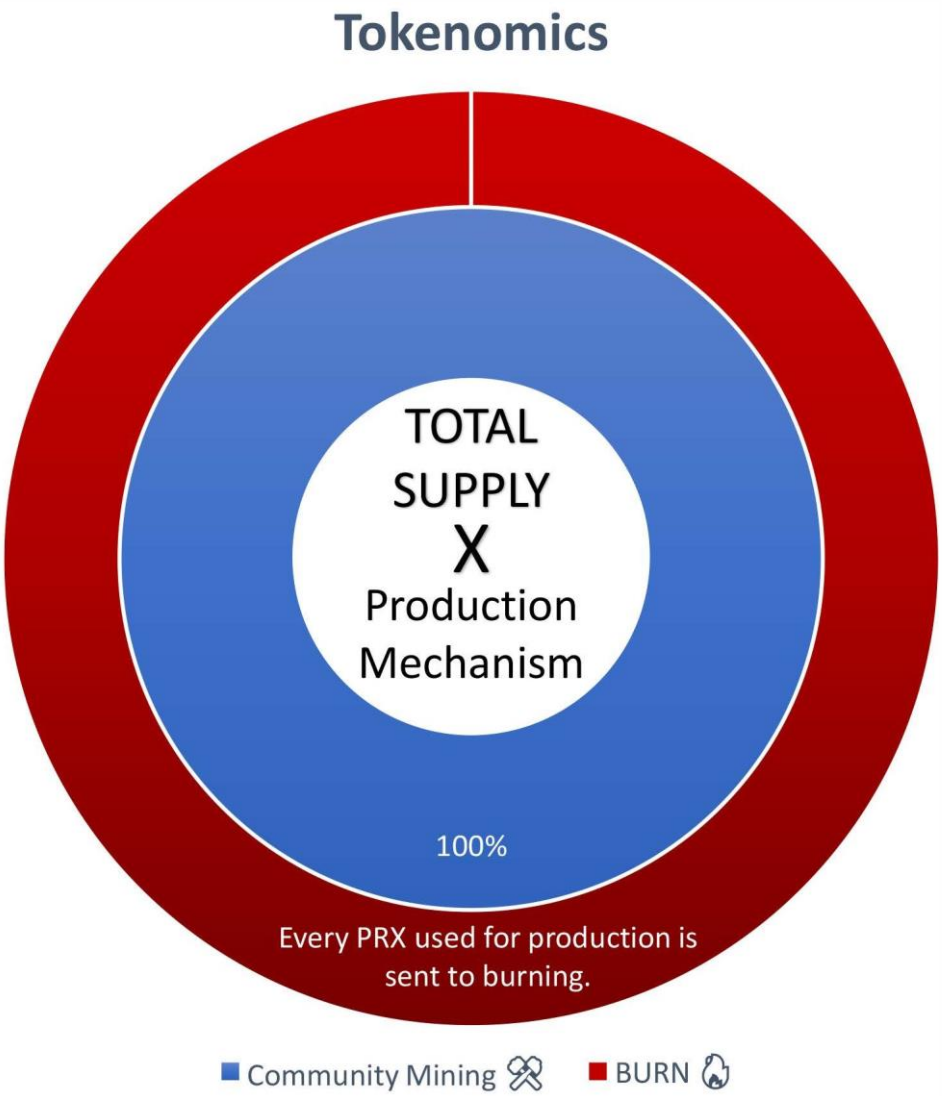


These service fees in the Parex production algorithm are fixed at certain rates considering the advantages of the users. These rates change during each halving process.

Incremental Service Fee rates:

- Start Mining = 5% - 25%
- First Halving = 1% - 18%
- Second Halving = 1% - 14%
- Third Halving = 1% - 10%
- Last Halving = 1% - 9%

11.6/ Tokenomics



Parex is a token whose entire supply is in the hands of its users. Distribution progresses through users. Production is done only by users. No PRX is produced outside of production.

11.7/ Proof of Interoperability

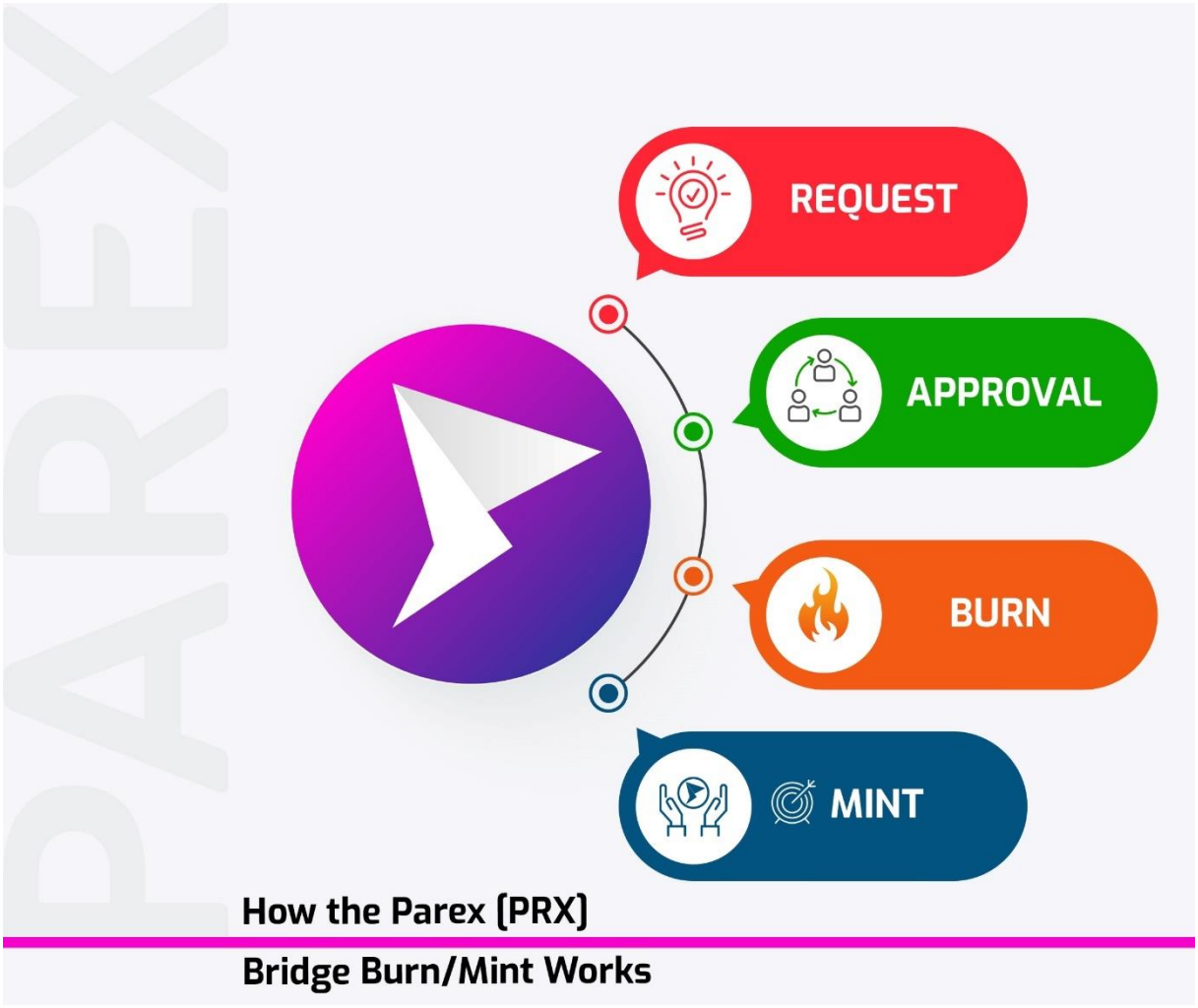
Thanks to Parex Proof of Interoperability, it establishes interoperable bridges with other networks. There is a balance between all networks. Circulation is common.

BEP20, ERC20, PEP20, Avalanche etc.

Burning is common. As soon as the PRX token is sent to production, it is burned and falls out of circulation. It continues its existence as a community- oriented project to overcome all difficulties.

The Proof of Interoperability mechanism ensures that the PRX token is an interoperable token in every network. In this way, every inter-network transfer is possible thanks to Parex Market. Switching between networks takes place at low fees and quickly through the Parex Market.

Bridge makes tiring routes easy for PRX.



Parex [PRX] is traded in many networks with a common circulation amount. With the unique bridge technology, burn in one network and mint in the other network takes place. In this way, the transfer between networks takes place quickly without changing the amount of circulation.

In order for users to transfer between networks at maximum speed, bridge transfers are made collectively at certain intervals. A certain amount of PRX tokens is transferred to the needed network. PRXs in the sending network are burned instantly. In this way, PRXs that users need for network exchange are in a position to be sent to user wallets quickly.

Parex Bridge transactions must be approved by PEP-2 validators (Master Tracker). A 51% approval is required for an inter-network transfer to take place. Transactions that do not receive 51% approval will not be processed. You can track network transfers and approval percentages at "bridgescan.parex.market".

PAREX BRIDGE APPROVAL PROCESS:

Parex creates a request for bridge transfer. Requests reach all Master Trackers as notifications via the Mobile App.

Master Trackers reach the "GUID" number of the requested transaction from bridgescan.parex.market address or via the command line below.

http://{DockerHostIP}:2020/getBurnApproveList/

The following command line is used to approve the request.

http://{DockerHostIP}:2020/setBurnApprove/{GUID}

12/ Website & Contact Information

Website: www.parex.market

Email: info@prxchain.com

13/ References

[1] Vasin, P. (2014) Blackcoin's Proof-of-Stake Protocol v2, https://blackcoin.co/blackcoin-pos-protocolv2-whitepaper.pdf

[2] A. Kiayias, I. Konstantinou, A. Russell, B. David, and R. Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. Cryptology ePrint Archive, Report 2016/889, 2016. http://eprint.iacr.org/.

[3] P. Daian, R. Pass and E. Shi, Snow White: Robustly reconfigurable consensus and applications to provably secure proofs of stake, Cryptology ePrint Archive, Report 2016/919, 2017.

[4] Rafael Pass and Elaine Shi. Thunderella: Blockchains with optimistic instant confirmation. https://eprint.iacr.org/2017/913.pdf.

[5] M. Zamani, M. Movahedi, and M. Raykova, “RapidChain: A Fast Blockchain Protocol via Full Sharding.” Cryptology ePrint Archive, Report 2018/460, 2018. https://eprint.iacr.org/2018/460.

[6] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, “Omniledger: A secure, scale-out, decentralized ledger via sharding,” in 2018 IEEE Symposium on Security and Privacy (SP), pp. 19–34, 2018.

[7] Loi Luu, Viswesh Narayanan, Chaodong Zheng, Kunal Baweja, Seth Gilbert, and Prateek Saxena. A secure sharding protocol for open blockchains. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS ’16, pages 17–30, New York, NY, USA, 2016. ACM.

[8] George Danezis and Sarah Meiklejohn. Centrally banked cryptocurrencies. In 23rd Annual Network and Distributed System Security Symposium, NDSS, 2016.

[9] The Zilliqa Team. The zilliqa technical whitepaper. https://docs.zilliqa.com/whitepaper.pdf, August 2017.

[10] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008. Available at https://bitcoin.org/ bitcoin.pdf.

[11] Miguel Castro and Barbara Liskov. Practical Byzantine Fault Tolerance. In Proceedings of the 3rd Symposium on Operating Systems Design and Implementation (OSDI ’99), New Orleans, Louisiana, February 1999.

[12] E. Kokoris-Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, and B. Ford. Enhancing Bitcoin Security and Performance with Strong Consistency via Collective Signing. In Proceedings of the 25th USENIX Conference on Security Symposium, 2016.

[13] Drijvers, M., Edalatnejad, K., Ford, B., & Neven, G. (2018). Okamoto Beats Schnorr: On the Provable Security of Multi-Signatures. IACR Cryptology ePrint Archive, 2018, 417.

[14] B. Alangot M. Suresh A. S Raj R. K Pathinarupothi K. Achuthan "Reliable collective cosigning to scale blockchain with strong consistency" Proceedings of the Network and Distributed System Security Symposium (DISS‘18) 2018.

[15] Baruch Awerbuch and Christian Scheideler. Towards a scalable and robust DHT. In Proceedings of the Eighteenth Annual ACM Symposium on Parallelism in Algorithms and Architectures, SPAA ’06, pages 318–327, New York, NY, USA, 2006. ACM.

[16] Vitalik Buterin and Virgil Griffith. Casper the friendly finality gadget. CoRR, abs/1710.09437, 2017.

[17] E. Syta, P. Jovanovic, E. Kokoris-Kogias, N. Gailly, L. Gasser, I. Khoffi, M. J. Fischer, and B. Ford. Scalable Bias-Resistant Distributed Randomness. In 38th IEEE Symposium on Security and Privacy, May 2017.

[18] The Ethereum Foundation. Ethereum Whitepaper. https://github.com/ethereum/wiki/wiki/White-Paper.