BLACK**PEARL.**CHAIN

Technical Whitepaper
version 1.0.1

BlackPearl.Chain ISSUER
Cayman Islands

Index

1. Introduction

A blockchain is a decentralized distributed ledger that combines data blocks in a chronologically end-to-end manner into a chained data structure that is cryptographically guaranteed to be tamperproof. Unlike traditional centralized databases, blockchains are fair, transparent, and tamperproof. It is this characteristic that gives the blockchain enormous potential in terms of technology and economy. It can be used in almost all industries, and it is the next-generation technological revolution after the Internet revolution.

With the development of digital cryptocurrencies such as Bitcoin, blockchain technology has received wide attention. Blockchain technology is a decentralized agreement, through data encryption, consensus algorithms and economic incentives, it has achieved a point-to-point transaction between nodes without mutual trust.

The introduction of the blockchain system supporting the smart contract represented by Ethereum has created new opportunities for the development of blockchain applications. Based on the trusted execution environment of the blockchain system, the smart contract platform enable complex operation of various digital assets on the blockchain, and open the door to rich decentralized application program (DApp). The development of digital currency trading system and smart contract application requires high performance and scalability of the blockchain system. However, the current mainstream public chain system has low performance and high cost, and it cannot provide fast and efficient services and a good user experience.

Blockchain technology can be of great value to all walks of life in both the technical and economic aspects. As long as there is a need to trust, blockchain technology can be used to build trust at very low cost and with high efficiency.

Blockchain technology has changed the production relationship. For thousands of years, transaction security has been guaranteed by reliable third-party intermediaries, such as banks, insurance companies, Alipay, real estate agents, etc., which help us build trust. Now we are able to complete transactions at a very low cost and with higher efficiency through blockchain technology in a peer-to-peer manner without the need for third-party intermediaries.

The blockchain market is a market of several trillions of dollars. Great changes in production relations and business models have happened. The centralized servers are the greatest value based on the traditional Internet-based centralized model. However, in the ecosystem of blockchain, the most valuable asset is the public-chain infrastructure which carries massive data, transactions and business activities, there is huge commercial value existing with public chain.

Over the past decade, blockchain technology has evolved over the following two generations:

The first generation of blockchain is a digital currency era represented by Bitcoin:
On October 31, 2008, Bitcoin founder Nakamoto Satoshi (a pseudonym) published a paper in the cryptography mail group - "Bitcoin: A peer-to-peer electronic cash system, and blockchain technology is the core foundation that supports bitcoin operations. Bitcoin does not require any third-party trust intermediary to operate safely for a decade, demonstrating that blockchain-based technology can establish trust between two unfamiliar individuals in a peer-to-peer manner and securely trade. Decentralized machine trust has withstood the test of time and hacking.

The second generation of blockchain technology is represented by Ethereum:
In 2013, the blockchain system proposed by Ethereum to support smart contracts created new opportunities for the development of blockchain applications. Ethereum has established a trusted execution environment based on blockchain technology. Smart contracts can control various digital assets on the blockchain to perform more complex operations and realize rich decentralized applications (DApp). This innovation makes many Commercial applications can be implemented based on blockchain technology.

At present, the industry encounters the dilemma that there is no good third-generation public chain, almost all the public chains that have been released fail to break through the "impossible triangle" (security, decentralization and performance). The first two generations of public chains are still in the prototype stage and do not have the basis for large-scale commercial applications.

The main problems are as follows:
The performance of the mainstream public chain is low. The TPS of Bitcoin can only reach 7 at the highest. The TPS of Ethereum can only achieve 10–20. The transaction is often severely blocked and cannot meet the needs of commercial landing.

The cost is high, the cost of a transaction usually exceeds the profit ceiling of most industries, limits the application to various industries, the value of the blockchain can not be realized.

The confirmation of a transaction is slow and does not provide immediate service and a good user experience. In the case of payment, Bitcoin payment requires one hour to complete, sometimes even one day if the congestion occurs, it is completely unacceptable for online merchant waiting for payments of the goods and services purchases.

Public chain comparison

	Block Produce Time	TPS	Consensus	Level of decentralization
ETH	15s	7	POW	Miner centralization
EOS	0.5s	28	DPOS	Representative Centralization
Gongxinbao	3s	<1	POCS (Proof of credit contribution)	Aliance chain
NEO	10s	<1	DBFT	Consensus node centralization
Qtum	1min ~ 4min	<1	POS	Centralization of rights by large capital holders
Bytom	30s ~ 7min	<1	POW	Miner centralization
ONT	1s ~ 15s	<1	VBFT	Large-cap mgt and equity centralization
ADA	20s	<1	POS	Large-cap holders and regional rights centralization

Since the industry does not have an ideal third-generation public chain release, some so-called “third-generation public chains” have emerged during the transition period. In fact, they belong to the alliance chain in essence, at the expense of security to obtain certain performance improvements, and the essence is that those implementations have not broken through the "impossible triangle”. These alliance chains should belong to the over-provisioning scheme. A small number of super-nodes have a large security risk and cannot be completely decentralized. Once a situation of cheating happens, it will cause loss of the user's digital assets and damage the credibility of the entire chain. And even worse, the credit collapses of those public chains actually can cause a huge negative impact on the entire blockchain industry.

The whole development of the blockchain industry depends on the real breakthrough of the public chain technology, solutions to the "impossible triangle", the reductions of the transaction costs. Only when those progresses happen, the blockchain technology can be landed on a large scale.

Here, we introduce BlackPearl.Chain, a third-generation public chain designed by BlackPearl.Chain Inc.

The entire BlackPearl.Chain is designed from ground up. It is totally different from Bitcoin, Ethereum and other public chain models. BlackPearl.Chain has solved the "impossible triangle". BlackPearl.Chain achieves superior performance through VRF lighting fast consensus, three layer sharding technique, threshold encryption, super secret private key, multi-dimensional routing, IPFS storage, system contract, and neuron node management.

BlackPearl.Chain can carry large-scale commercial applications with super low gas fees in order to help wide range of industry applications to land on blockchain technology.

2. BlackPearl.Chain Technology breakthroughs

BlackPearl.Chain can effectively support huge volume of small amount real-time payment, decentralized digital currency trading, instant messaging, e-commerce, search, notarization, social, media, digital assets, traceability and so on.

BlackPearl.Chain is fully decentralized with linear expansion capability, it can support tens of millions of TPS with the increase of nodes. It's extremely secure, and resistant against quantum computation and biological computation.

BlackPearl.Chain has made innovative breakthroughs in consensus, computing power, storage and communication. It is fully scalable, provably secure, and energy efficient. Specifically, BPChain makes breakthroughs in following aspects:

- **Fully Scalable with Intelligent sharding:** It has innovative three-layer sharding design, completely solves trust between shards. It also provides asynchronous sharding consensus, inter-shards communication. The ai capable loading balance algorithm of data collection and distribution can automatically complete sharding and merging. The performance of the public chain can be infinitely improved by this breakthrough, enable BlackPearl.Chain's performance to exceed the performance of the centralized server.

- **Secure and Fast Consensus:** BlackPearl.Chain implements VRF lightning fast consensus. Its unique VRF implementation randomly selects current round of voting nodes, achieves pioneered lightning consensus. It only requires 0.3 seconds - 3 seconds to complete consensus.

- **Computing power reduction:** With BlackPearl.Chain, APP is a node. This technology fully organizes and utilizes the global idle computing power and bandwidth, enables building powerful computing and storage capabilities without incurring extra huge expenses on professional mining machines. Users can install BlackPearl.Chain wallet to participate in consensus and block production.

- **Improved Network Performance:** Super-routed P2P broadcasts enable current home broadband to achieve up to several thousand single-Shard TPS. (At current broadband conditions, the measured TPS peak is 5730)

By innovating on both the protocol and network layers, BlackPearl.Chain provides the world with a scalable and secure blockchain system that is able to support the emerging decentralized economy. BlackPearl.Chain will enable applications which were not previously feasible on blockchain, including high-volume decentralized exchanges, interactive fair games, Visa-scale

payment systems, and Internet-of-Things transactions. BlackPearl.Chain strives to scale trust for billions of people and create a radically fair economy.

3. Blockchain fundamental challenges and BlackPearl.Chain's approach

3.1 Blockchain History Review

A brief review of the blockchain history will help to understand the revolutionary nature of the BlackPearl.Chain.

In 2008, Nakamoto published a famous paper, "Bitcoin: Peer-to-Peer Electronic Cash and Gold System". In January 2009, the Genesis block was mined. "The Times Jan 03, 2009 Chancellor on brink of second bailout for banks." Like a magic, it started the era of bitcoin blockchain. In 2013, Bitcoin released the most important version in its history. This version optimized the Bitcoin node's internal management and network communication, and Bitcoin as digital currency started to cause global impact. Bitcoin was a great success as the first crypto digital currency, but the poor scalability of Bitcoin drastically constrained the subsequent adaption of the blockchain. Bitcoin represent the 1.0 era of blockchain. In order to solve the problem of scalability of Bitcoin, Vitalik Buterin invented Ethereum. Ethereum has a clear design and system architecture, from EVM papers to ICO framework, from different versions of POC to 2015 Frontier stage, from PoW's Metropolis stage to PoS's Serenity stage, The Turing completeness of Ethereum, smart contracts platform, resistance to ASIC design and blockchain applications are the main hallmarks of the blockchain 2.0 era. Ethereum provides a platform interface and programming language that enables developers to build and publish next-generation distributed applications. The later story following is well known. In February 2018, the bitcoin computation powers reached 20EH/s, and On Github, more than 90,000 open source projects are blockchain related. More than 90 countries including China, the United States, the United Kingdom, Singapore, Russia, Japan, and South Korea have joined the research on blockchain technology. From 2008 to 2018, the ideas and rationale of the blockchain were digested, explored, and practiced by the general public. All this happened within only one decade. Compared with the development of the Internet, one can see the success of the blockchain: In 1974, the United States Department of Defense National Defense High Research Institute (ARPA) development announced the TCP / IP protocol, marked the first year of Internet era. In 1994, after 20 years, China officially entered the Internet era.

3.2 BlackPearl.Chain Approaches to two major challenges of Blockchain

3.2.1 SHD completeness

In a distributed system, Consistency, Availability, and Partition tolerance are not achievable at the same time, this is called CAP theorem. Nakamoto's blockchain relies on Probabilistic Strong Consistency to achieve a consensus which is called the Nakamoto consensus. In the blockchain system, similar to the CAP theorem, Security ("S"), high performance ("H") and Decentralization ("D") are not achievable at the same time. It's called SHD completeness issue. Under the premise of inefficient CPU power, Nakamoto proved that the security "S" and the decentralized "D" were able to coexist, but, the high-performance "H" was sacrificed. Due to the consensus algorithm and the design of capacity of each block, an average of ten minutes is needed for Bitcoin to produce a block, and only seven transactions can be processed in one second. Not only that, with the advent of high-performance "ASIC mining machines", the probability of ordinary CPU computing power gaining benefits from Bitcoin is reduced to zero, the mining machine easily obtains super-linear benefits, lately, the emergence of mines and mining pools completely broke the center of Decentralization, and now, the Bitcoin is clearly not an equal participation community. To make matters worse, the mines and the mining pools continuously monopolize the computing power. It's possible that a small number of participants eventually can own more than 51% of the computing power, and the safety "S" will not be guaranteed. Therefore, we say that the blockchain of Bitcoin has lost the balance of SHD.

In order to avoid the devastating effects of the ASIC mining machine, Ethereum adopted the ASIC resistance algorithm of "repeated read cache", which maintained the security "S" and the decentralized "D" in a short time, but "CryptoKitties" , the first large-scale smart contract application on Ethereum has completely collapsed the Ethereum system, and the high-performance "H" is particularly low. So, the latest consensus trend has turned to PoS or DPoS from PoW. The blockchain system that has turned to the PoS or DPoS consensus has greatly improved the system performance, but has neglected the fundamental meaning of decentralization, and the system has been mastered by a few stakeholders. The direction of the development side is not much different from the existing centralization system.

By designing a VRF-based consensus mechanism, BlackPearl.Chain adopts a system in which all nodes can participate to ensure that the Token holders have their own rights and interests, while improving safety as well as improving high efficiency, the basics of decentralization is also maintained, thus BlackPearl.Chain has achieved the completeness of SHD.

3.2.2 Balanced value transfer

The era of the Internet has changed the way and the rationale of information transmission. People use the Internet technology to transfer information conveniently and at low cost. Internet has enabled the exponential level improvement of efficiency and costs reduction, and people have gained unprecedental new product experiences and services. However, the concept of information transfer and value transfer is different. The Internet network does not have the peer-to-peer value transfer function. The value transfer depends on the central office to undertake the bookkeeping function, because the value transfer needs to guarantee the unique one. This is not the same as the reproducibility of information transfer. By using distributed shared accounting technology, Bitcoin establishes a decentralized trust, no longer relies on the centralized organization, and thus supports peer-to-peer value transfer, changed the value transfer and pricing rules. Due to the emergence of the mining pool, the value transfer of Bitcoin has been tilted, and the accessibility to value by ordinary participants and by mining machine owners is no longer equal, and the value is quickly concentrated in the mining pool. Ethereum resists this inequality through ASIC resistance algorithm and utilize “Gas” consumption to suppress the resources on the chain, thus slowing down the value accumulation of the mining machine to a certain extent. However, we think this is a negative and short-term practice, it does a poor job to support the long-term growth of blockchain development. The PoS or DPoS consensus attempts to achieve equilibrium by breaking the PoW computing power monopoly, but the powerful Token owners still have a value orientation, and the centralization is more concentrated than PoW. According to the current development of the blockchain and cryptocurrency, the value is concentrated in the hands of a few people in a way that mimics the 80/20 law.

BlackPearl.Chain team aims at changing the way of existing value transfer, let the value completely flow openly, and providing users with a balanced value transfer system. BlackPearl.Chain team believes that each individual is both a provider and a buyer of the service, that is, the buyer is also the seller. The center value of the decentralized market is the price adjustment mechanism, and the price will be reached in a dynamic equilibrium way. BlackPearl.Chain uses the idea of average field game theory to study price dynamic fluctuations. There should be a positive correlation between rights and interests, but it is not a linear relationship, thus inhibiting the excessive concentration of power. BlackPearl.Chain has created a new generation of balanced value interconnection system. The system will bring a major revolution in business models and society economically.

4. BlackPearl.Chain Designers

BlackPearl.Chain designers and builders come from top Internet companies, universities and research institutes. The team consisted of mathematicians who incorporated the results of game theory into the blockchain, as well as communications experts, computer experts, economics experts, and philosophers. All the theoretical design of BlackPearl.Chain adopts a two-validation process: first, the mathematician completes the consensus modeling and numerical simulation experiment; and then the computer and communication experts make the actual verification of the theoretical design of the BlackPearl.Chain project with strict standards.

The current work results of BlackPearl.Chain project are attributed to the close cooperation and joint effort between theory and experiment, software and hardware. The VRF consensus mechanism was designed by experts from the fields of mathematics, communication, and computer.

Major contributors:

60+ contributors, collectively owns more than 60 years expertise at: Apple, Cisco, Microsoft, Baidu, Tencent, Amazon, Banking industry; cryptography, Security, distributed system, computer network, system design, system architecture, AI, data mining, deep learning, machine learning, embedded OS, storage, network traffic, security development of AI model, system security, distributed architecture stability; ACM algorithm, golang, C++.

5. BlackPearl.Chain System Design goal and core solutions

5.1 Design goal

The BlackPearl.Chain team designed and developed the next-generation public chain that can carry large-scale commercial applications, meeting the following objectives:

- Fully decentralized; linear expansion; support for tens of millions of TPS with the increase of nodes; confirmation in seconds; extremely secure; resistance of quantum computing and biological computing attack; no waste of electricity resources; ultra-low Gas fee; Turing complete Smart contract platform.

- With VRF consensus and unique economic incentive model, create balance of each individual's economical right and interest, integrate game theory into the blockchain to create SHD completeness.

- Support Billions of users and Trillions of devices to use BlackPearl.Chain simultaneously.

5.2 Core solutions

In the current Ethereum design implementation, all consensus nodes store a complete blockchain, which stores all transaction states. This guarantees the safety of Ethereum, but it also limits the scalability of the blockchain. When the system's processing power is increased, massive data storage will limit the participation of ordinary users.

System Scalability: BlackPearl.Chain used a sharding technical solution to solve the scalability problem. As the number of nodes increases, the computational power of parallel computing increases, and the processing power of the system increases.

Storage solution: Data distributed storage technology is adopted to solve the storage problem of block data under high concurrency. Designed to solve the full expansion issue of blockchain by

adding collecting nodes, sorting centers, super storage nodes, and storage sharding technique.

With scalability and storage solution, tens of millions TPS can be achieved.

6. System architecture

6.1 System layer

The system architecture of BlackPearl.Chain consists of the application layer, contract layer, incentive layer, consensus layer, network layer and storage layer.

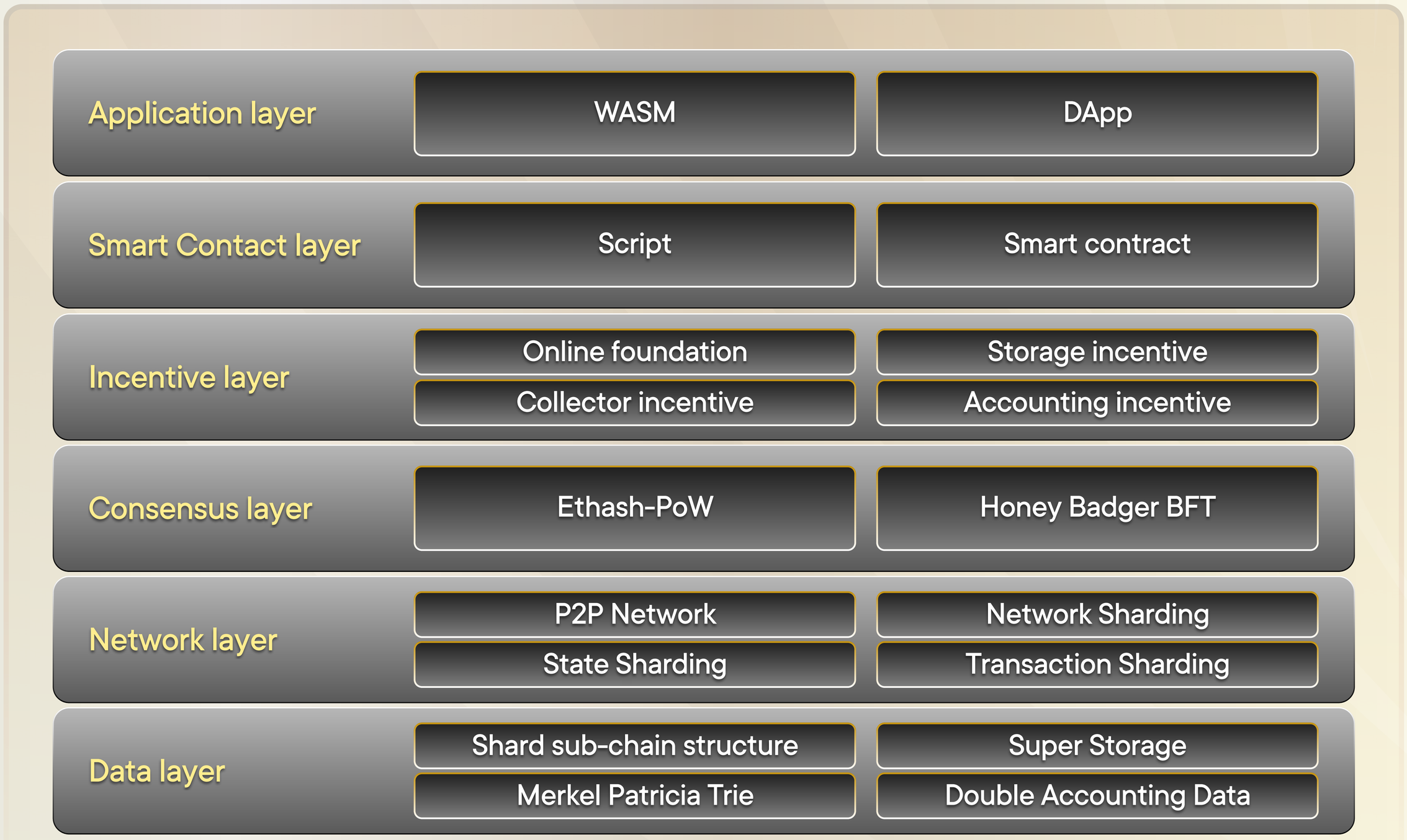

Fig. 6.1: SYSTEM ARCHITECTURE

6.2 The node architecture

Fig. 6.2: THE NODE ARCHITECTURE

6.3 Transactions between Shards

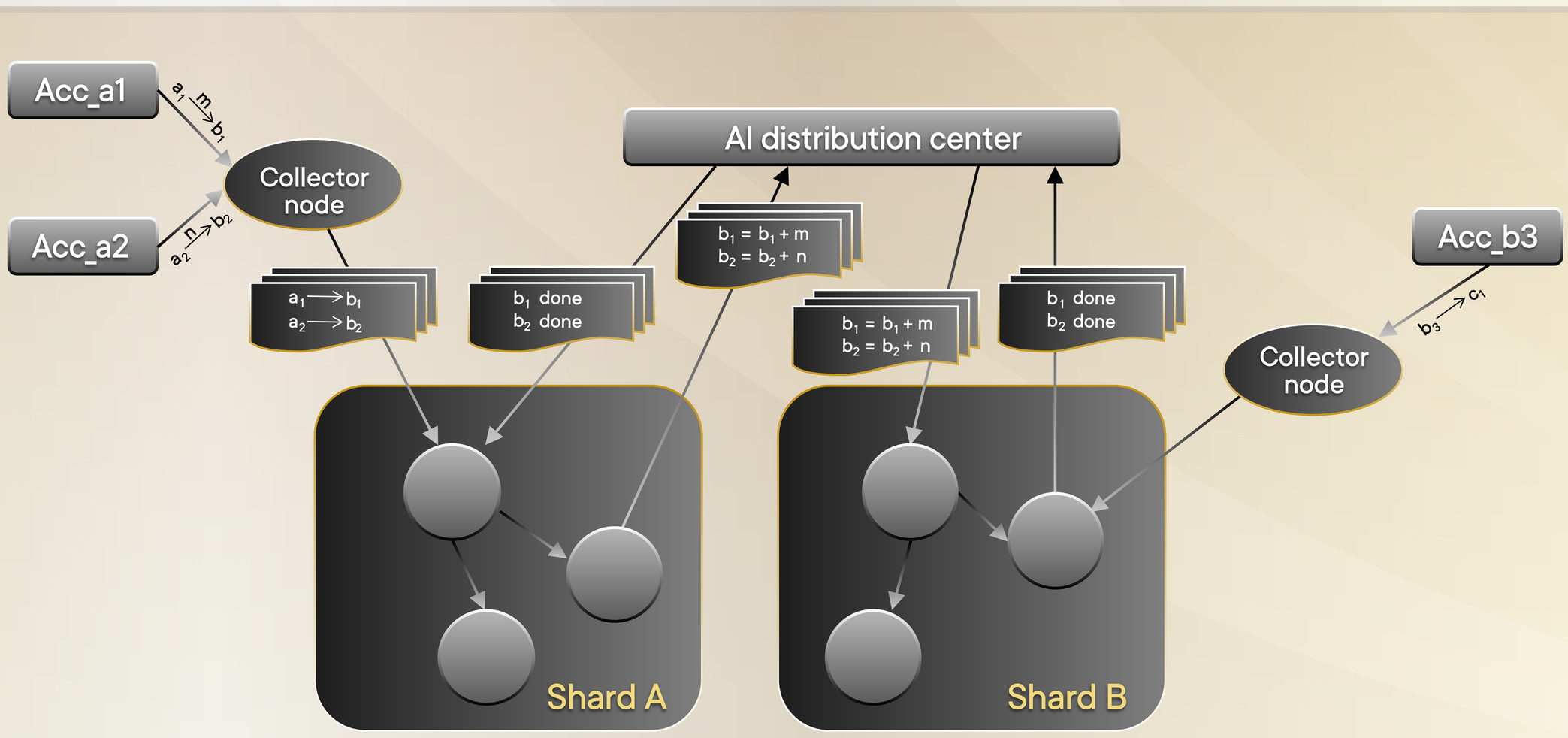

Fig. 6.3: TRANSACTIONS BETWEEN SHARDS

6.4 The Incentive Model

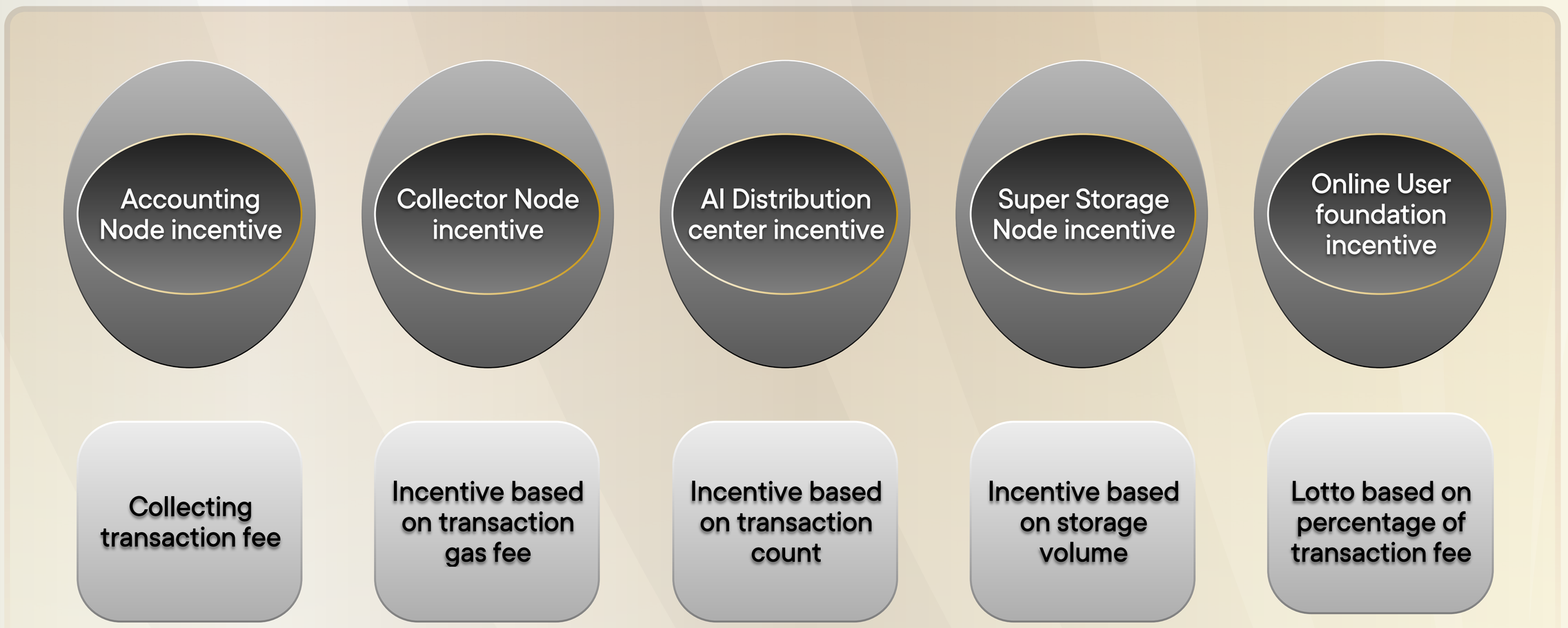

Fig. 6.4: INCENTIVE MECHANISM

6.5 The system components

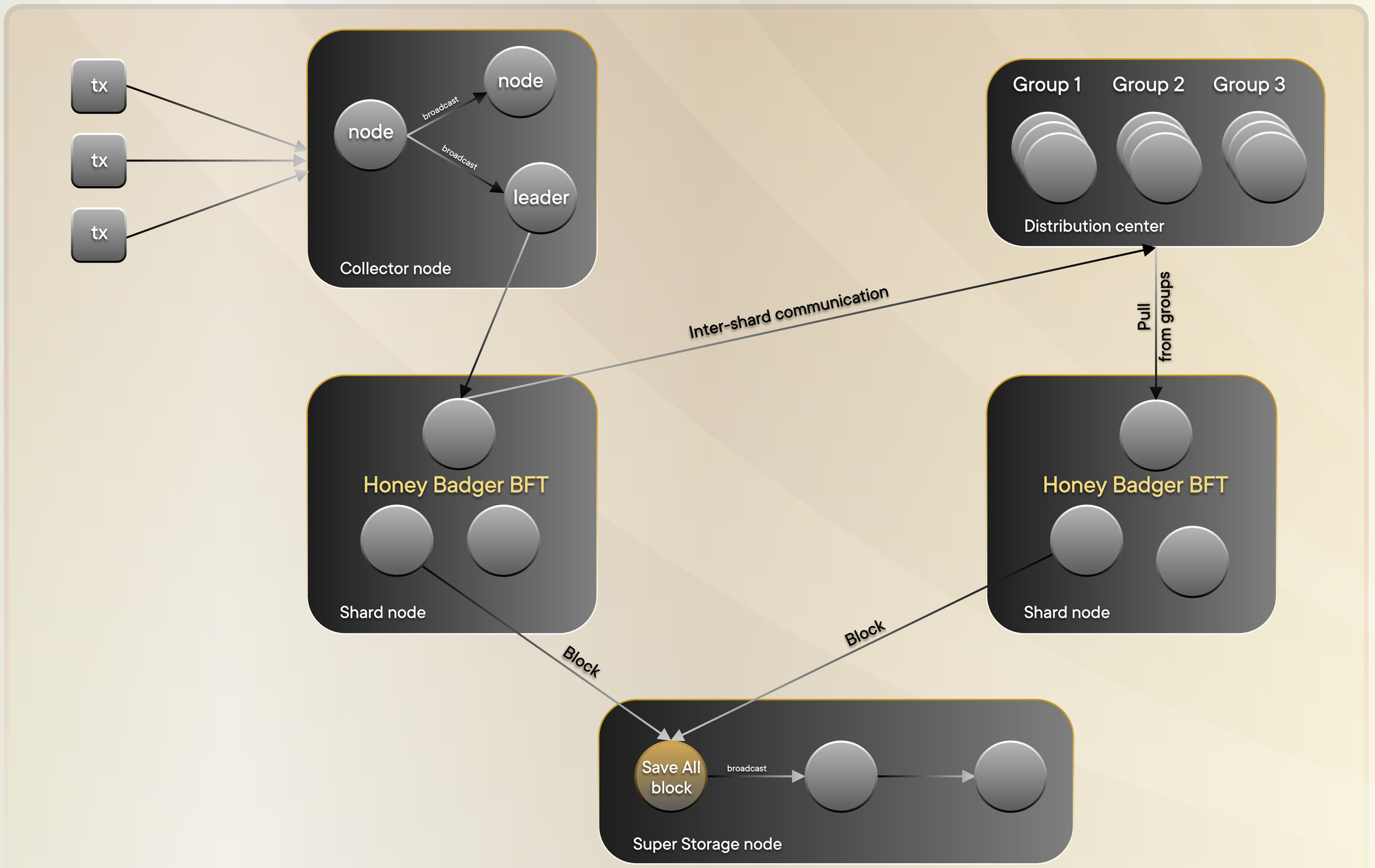

Fig. 6.5: SYSTEM COMPONENTS

As shown in Fig. 6.5, there are four different types of nodes in the system:

- **Collector**

The collection node is responsible for collecting transactional information and forwarding it to the specific accounting node of the corresponding shard. Collection nodes can reduce the number of network communication by aggregating transactions, and improve the network efficiency.

- **Sharding node**

Different sub-shards are mined in parallel, each shard reach consensus internally. Each shard simultaneously stores part of the blockchain data to reduce the storage load of the nodes within each shard.

- **Distribution center**

Transactions between shards need inter-shard communication, distribution center is introduced to solve inter-shard communicaton. The distribution center forms groups of transactions according to the receiving party of the transaction, and the receiving shards actively pull the the data from respecting group.

- **Super storage node**

Since each node of the shards only stores part of the ledger data, sometimes, some of the nodes are offline, in order to obtain the shard data, or query the on-shard contracts, the super storage node is introduced to store all the blockchain data.

7. Transaction process

The transaction submitted by the user is collected into the transaction pool, verified by the VRF consensus, packaged, and exported, and the p2p synchronization is completed before the transaction is confirmed.

The entire transaction process is divided into 7 steps. Before the transaction is conducted, the system must ensure that the various types of nodes in the network have been elected through consensus. Steps are as shown in Figure 7-1.

1. First, the system generates the collection nodes, the sharding nodes, the sorting center and the super storage nodes required in the network through the consensus algorithm;

2. Client A initiates a transaction, for example, starts a transfer of 1 unit currency from address A to address B. Client A which initiates the transfer needs to construct a transaction, and to sign the transaction;

3. The transaction initiated by client A and transactions initiated by other clients use a routing mechanism to select the nearest collection node for sending the transaction, and after the collection node receives multiple transactions sent by various clients. it will hash the transactions and find out the destination shard for each transaction, transaction with the same destination shard will be assembled into one package. The collection nodes send the transaction packs to the neighboring collection nodes through a broadcast, and the collection node leader forwards the transaction packs to the corresponding target shard. The collection node leader is responsible for maintaining the route towards the target shard, and collection node leader will be rotated according to the round-robin method;

4. Assume that the transaction initiated by client A is hash to the shard J according to the address A. After the shard J receives the transaction package forwarded by the collection node leader, the transactions within the transaction package will be taken apart and be added to the unconfirmed transaction pool of the shard node, and the transaction is widely broadcasted in the shard. The shard node ranks the transaction priority according to the gas in descending order, and selects the transaction in the unconfirmed transaction pool to be packaged. The shard node first reduces the balance of the address A by 1 unit coin, and then sends a request for increase the balance of the address B by 1 unit coin to the distribution center;

5. After receiving the balance increase operation request for the address B forwarded by the shard node leader in the slice J, the distribution center adds the request to the address B to the corresponding transaction processing queue of shard K according to the same hash algorithm as the collecting node. Also, the distribution center adds the requests for the shard J and other shards to the corresponding transaction processing queues of those shards, waiting for each shard node leader to pull the message from the corresponding queues;

6. In the shard K, the shard node leader periodically pulled from the distribution center to extract the transaction package from the processing queue, and broadcasts the transaction package to other nodes of the shard. When a shard node receives an operation request for the address B to increase by 1 unit of currency, the balance of the address B is increased by 1 unit of currency, and the transaction for receiving 1 unit of the address A by the address B is added to the processed transaction pool. And the shard node performs the accounting and producing new block according to the consensus algorithm for the shard. The shard node leader in the shard K sends an operation completion request for increasing the address B balance by 1 unit coin to the distribution center;

7. After the distribution center receives the request from the shard J node leader regarding to the processing completion of 1 unit currency increase for address B, it adds the request to the pending processing queue of shard J which is corresponding to the address A;

8. In the shard J, the shard node leader periodically pulls the transaction package from the corresponding transaction processing queue for shard J from the distribution center, and broadcasts the transaction package to other nodes within the shard J. When a certain shard node processed the completion request of increasing 1 unit currency for address B, the transfer transaction is added to the processed transaction pool. Finally, the shard node performs accounting and producing new block by using the consensus algorithm for the shard.

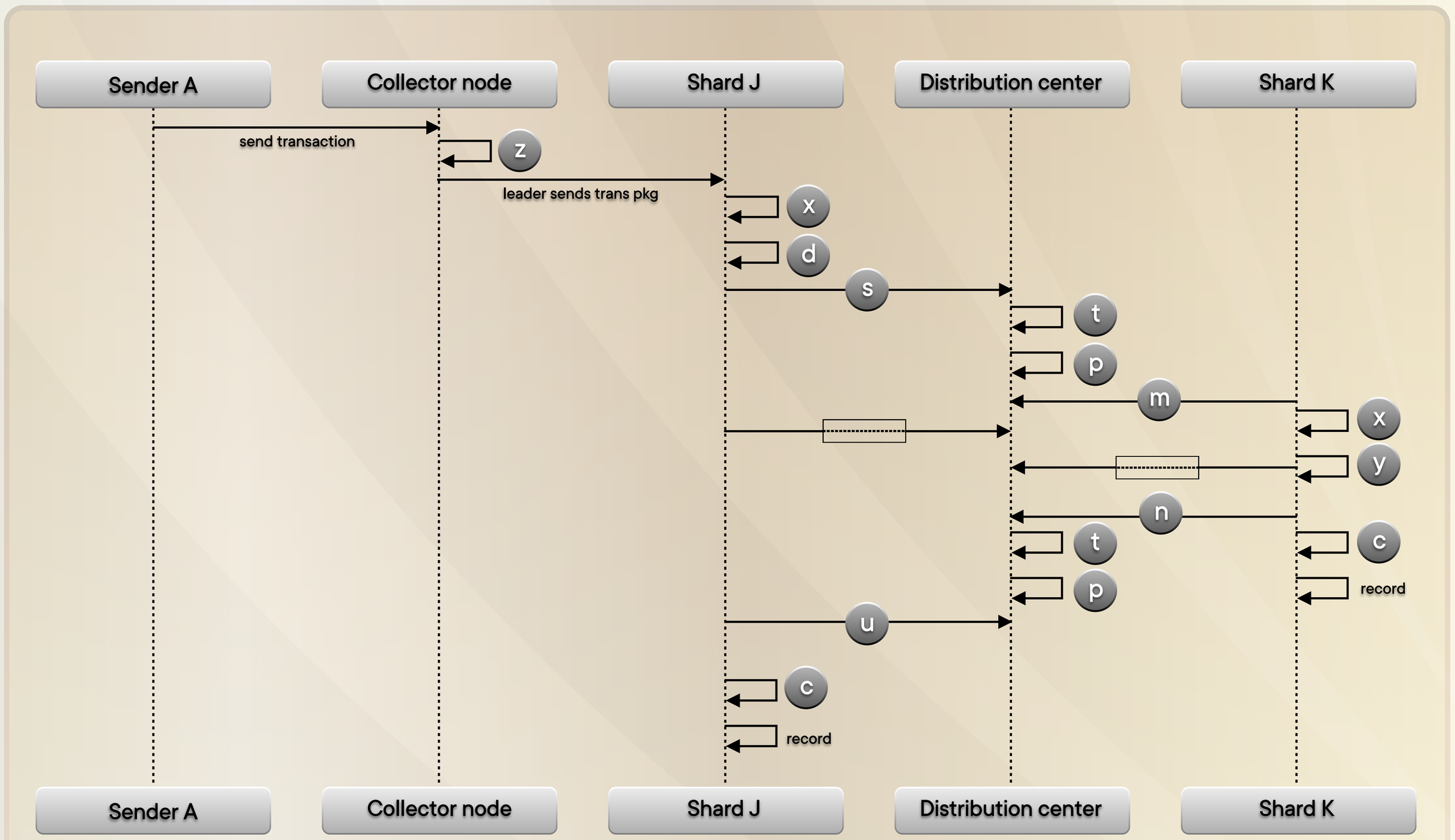

Fig. 7.1: TRANSACTION PROCESS

8. Sharding

Blockchain sharding as a scalability solution has gained lots of attention since late 2017. With Sharding technology, as the number of nodes increases, the computational power of parallel computing increases, and the processing power of the system increases.

With sharding mechanism, BlackPearl.Chain had improved transaction efficiency, reduced computing power, and reduced storage pressure. BlackPearl.Chain sharding mainly includes network sharding, state sharding, and storage sharding.

8.1 Network sharding

The network sharding mechanism completes the transaction pool synchronization, consensus, and block producing within the shard, and the parallel computing is performed on multiple shards. The performance of the parallel computing increases with the number of participating nodes.

The network sharding divides the entire miner network into four types of nodes, namely the collector node, the shard node, the distribution center and the super storage node described above.

Super Storage Node

The Super Storage Node is maintained manually in the configuration of each miner node. In principle, every miner node can access the super storage node to get the global block ledger.

Election of distribution center node

The miner's network uses Ethash-PoW for the election of the distribution center nodes. The nodes that complete the Ethash-PoW calculation are arranged in descending order of nonce size. The first 2nh nodes are selected into the candidate node pool, and the nodes in the candidate node pool are sorted in descending order according to bandwidth, available memory, CPU, and disk speed, and the first nh nodes are selected as the distribution center node. Also, the distribution center node determines the number of shards per nh/20, maintains the message to be processed by shards in the distribution node memory.

Election of shard node

After completing the election of the distribution center node, the miner network will elect the shard node through Ethash-PoW and submit to distribution center for verification. The nodes that complete the Ethash-PoW calculation in this round are ranked in descending order of nonce size. The first nh*ns/20 nodes are selected as the shard nodes, and every ns shard node in one shard.

Election of Collection Node

The miner network will elect the collector node through Ethash-PoW and submit to distribution center for verification. The nodes that complete the Ethash-PoW calculation in this round are ranked in descending order of nonce size. The first 10*nco nodes are selected as the collection node, each 10 collection nodes are clustered. The collection node is used to package the transaction and to send the package to corresponding destination shard.

8.2 State sharding

The state sharding divides the balance and smart contract state information corresponding to each address into corresponding shards. For example, the state information of the address A is maintained in the shard 1, and the state information of the address B is maintained in the shard 2. When address A initiates a transfer transaction to address B, the balance of address A at shard 1 reduces and the balance of address B at shard 2 increases. The communication between shards is performed by the To-be processed message queue in the distribution center, and the shard pulls the To-be processed message queue from distribution center and send complete request to distribution center when operation completes.

Each shard produce a separate chain, and only the transaction hash is recorded to the chain for the shard, as shown in Figure 8–1. To access the complete transactional information, one needs to visit super storage node. The whole miner network will generate same number of sub- chains as number of shards.

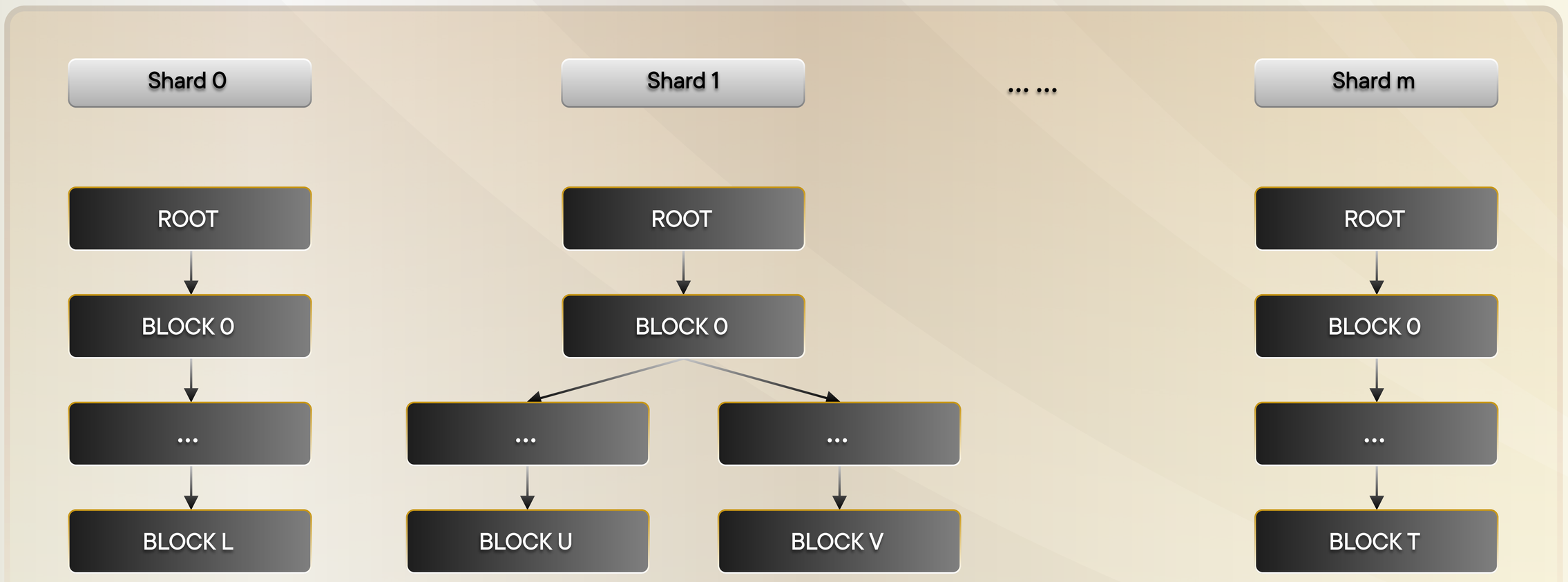

Fig. 8.1: SUB-CHAIN FROM EACH SHARD

8.3 Storage sharding

Each shard, only store transaction data within the shard, in this way, it reduce the pressure of storage through distributed storage schemes.

9. Consensus algorithm

9.1 Design assumption

9.1.1 The number of honest nodes in the network is always dominant.

9.1.2 Nodes are free to join the network at any time without having to apply.

a.) In BlackPearl.Chain network, each node is represented by a public key address (also a wallet address). For the newly added node address, only after other nodes in the network successfully transfer to the newly joined node (that is, the wallet balance is greater than n=100), it then can participate in the block producing consensus in the network.

b.) In order to prevent malicious registration, each joiner needs a waiting period and completes a POW workload proof before it can participate the consensus process.

c.) The PoW workload contains performance tests, including computing power, bandwidth, internal and external storage speed, and capacity.

9.1.3 The attacker is also dynamically changing (honest nodes can become attackers at any time).

9.2 BlackPearl.Chain Consensus

BlackPearl.Chain adopts and upgrades VRF (verifiable random function) consensus. The introduction of VRF consensus makes the election process unpredictable and unmanipulable. The selected nodes complete the shard consensus and block producing work, and do not need full participation from all blockchain nodes. Performance does not decrease as the number of members on the shard increases.

The consensus solution improves the efficiency of the block producing, improves the throughput, and allows the computing power focus on effective operations such as verification, comparison, and block producing. It reduces the waste of social resources associated with PoW consensus.

BlackPearl.Chain VRF lightning fast consensus is a completely new consensus protocol that can quickly converge, calculate states and reach consensus right away. This mechanism is fundamentally different from the traditional VRF.

The traditional VRF uses a random function to draw a lottery to form a committee, and the consensus is reached by communication between the committee members. It is relatively easy to influence the fairness and to reduce efficiency through communication disruption, isolation, and bribery. BlackPearl.Chain has utilized relay broadcasting, multi-signing, state switching techniques. Through our proprietary unique algorithms and processes, BlackPearl.Chain has addressed the traditional VRF issues.

The consensus algorithm for each shard uses the Honey Badger BFT consensus to better follow the network state in the asynchronous network and reduce communication overhead. The consensus algorithm running process is divided into 11 steps.

9.2.1 The shard leader starts the current epoch, in which N nodes exists, and each node in the shard randomly selects B/N transactions from the transaction queue, (B is the overall batch size), using the public key to conduct encryption with the threshold encryption algorithm;

9.2.2 Each node will broadcast the self-encrypted transaction package to other nodes, and also broadcast the BVAL message to vote for the transaction package.

9.2.3 If the node receives the BVAL message sent by other nodes, it immediately responds to and votes for the BVAL message;

9.2.4 If the node receives BVAL message from f+1 nodes which carries either vote for or rejection message , and if the voting content received is different from the node's previously sent one, the same voting message as f+1 nodes is sent;

9.2.5 If the node receives the vote for or vote rejection message sent by 2f+1 other nodes, then it broadcasts AUX message with the same voting content as the incoming message ;

9.2.6 If the node receives the vote for message sent by N-f other nodes, it sends a vote rejection to other nodes.

9.2.7 The node waits for the network to respond to N-f AUX response messages, setting the vals value to the majority of the votes in the AUX response message.

9.2.8 The node gets the coin value S of this epoch, if the majority voting of AUX message matches the majority of the voting of BVAL message and if the result is the same as the coin value S, then the node's broadcasted encrypted transaction package will join the ACS (asynchronous Common subset);

9.2.9 Each node performs the threshold cooperated decryption of each transaction in the ACS, and broadcasts the decrypted result to other nodes;

9.2.10 The node waits to receive f+1 decrypted results, and decrypts the received decrypted result by using public key with the threshold decryption algorithm. The end result will be the original transaction. And the original transaction is de-weighted and sorted, this becomes the final transaction to be recorded.

9.2.11 The shard leader will produce the block including transaction from above step and write it into the sub-chain of the current shard.

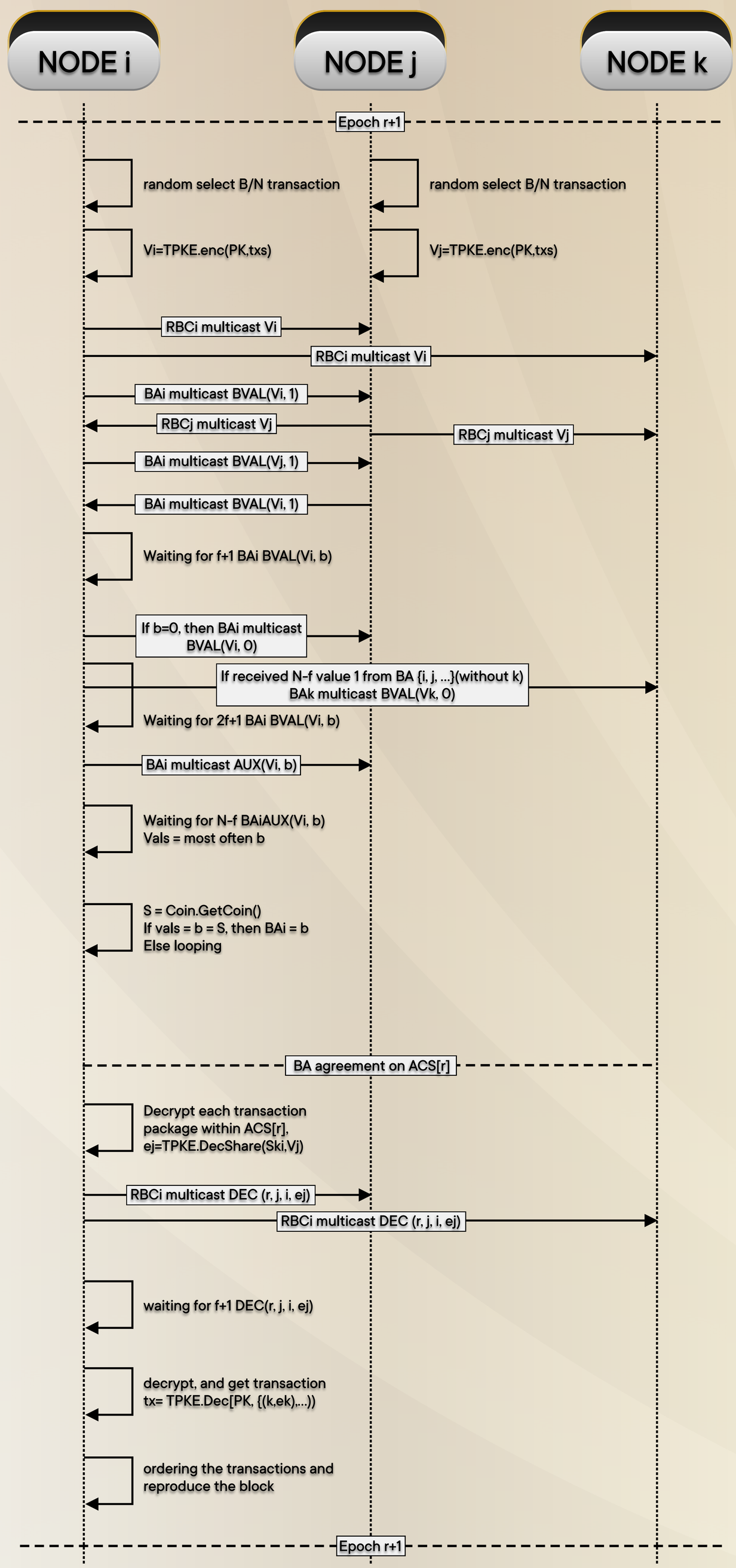

Fig. 9.1: HONEY BADGER BFT CONSENSUS

10. Storage System

10.1 The block structure

Each block is made up of multiple transactions. Let's first look at which fields a transaction contains. The trading account uses Ethereum's account system instead of Bitcoin's UTXO (Unspent Transaction Output). A transfers money to B. The most basic fields are A's account number, B's account number, and the amount of money transferred. Bitcoin uses UTXO to solve the double-flower problem, and each unspent output can only be referenced once. Similar to the Ethereum account system, in order to solve the double spending and replay attacks, a nonce field is introduced. Each account has a nonce field. For each transaction sent, the nonce will be automatically incremented by 1.

Also borrowed from Ethereum, BlackPearl.Chain introduces gas. The price of the token on the market is constantly changing, and the computing resources required for the execution of smart contracts are relatively fixed, so gas is introduced to measure computing resources. After the introduction of gas, you need to add a gas_limit parameter to defend against attacks, prevent hackers from executing smart contracts with infinite loops; also, keep the processing time of smart contracts at a low level and improve the trading efficiency of the system.

In summary, a transaction contains the following fields:

from: the sender address of the transaction
to: the recipient address of the transaction
value: the number of digital currencies transferred
nonce: a mark that distinguishes same users from different transactions.
gas_price: the price of the gas the sender is willing to pay
gas_limit: the maximum amount of gas that can be consumed by executing a transaction

After the transaction is generated, the transaction needs to be signed, first being hashed and then, being encrypted with the private key.

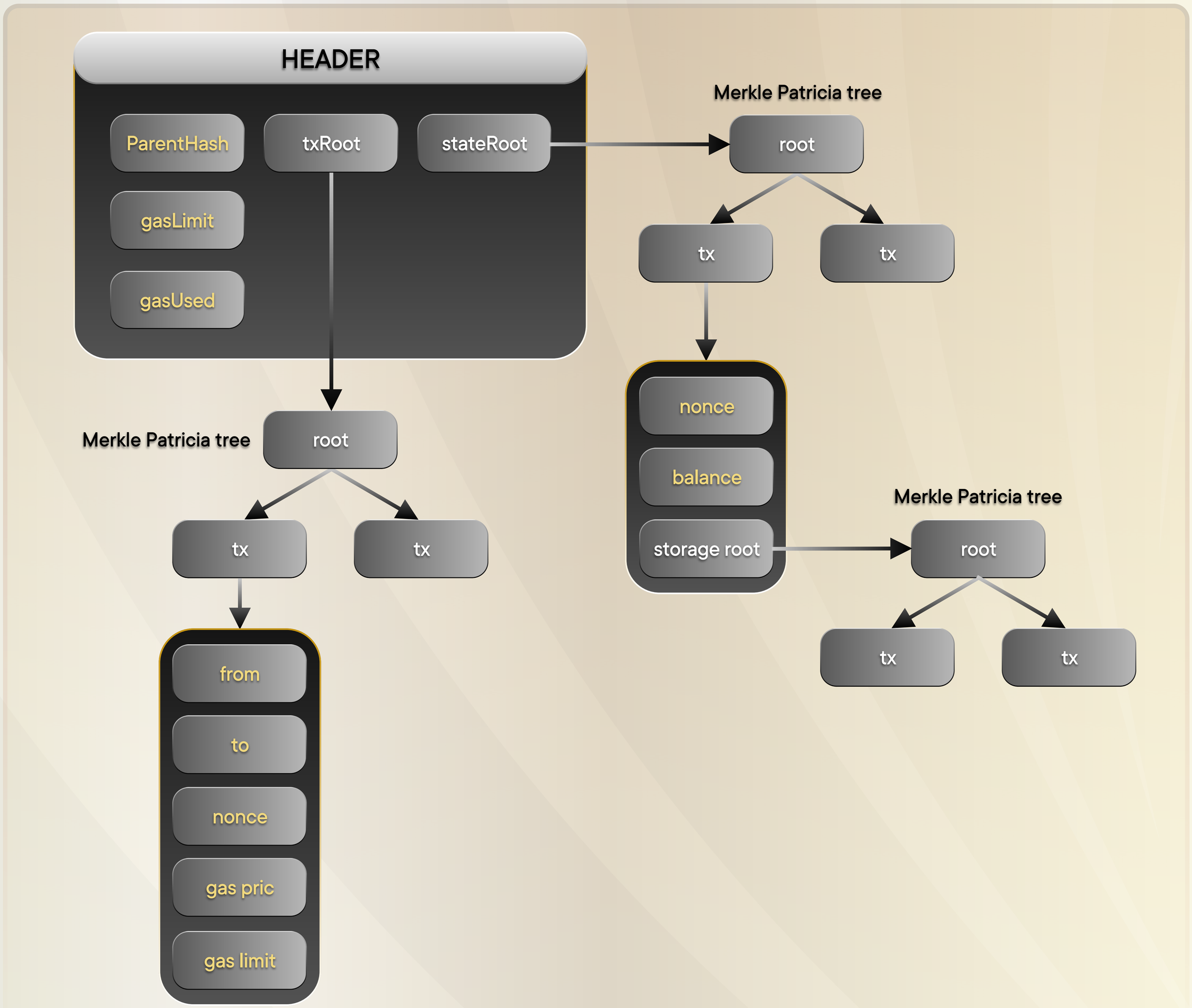

Fig. 10.1: BLOCK STORAGE STRUCTURE

Bitcoin uses the Merkle tree for transaction storage. The advantage of using Merkle tree is that it is easy to verify the integrity of the entire block by comparing the root hashes. When it is necessary to verify whether a block has been tampered with, it only needs to extend from the current block to the root node to calculate the hash of a small part of the node. When adding a new node, you do not need to recalculate the hash of all the blocks, just recalculate the hash of some nodes.

10.2 The state structure

After adding the account system, each user's state contains the following data:
nonce: the number of transactions sent from the current address
balance: the balance owned by the current address
storageRoot: contract data

Different from historical transaction data, the user's state data needs to be updated frequently. Every time a transaction is initiated, the nonce and balance under the account need to be updated. Also, new users are constantly added to the network. In order to facilitate the query of the balance of a certain user, an efficient data structure is needed to support fast search, addition and modification of account data, and it is necessary to ensure that the data is easy to verify and prevent data from being tampered with. Ethereum has proposed an improved Merkle Patricia tree, and the BlackPearl.Chain public chain will also use the Merkle Patricia tree to store state data and transaction data.

The specific structure is shown below:

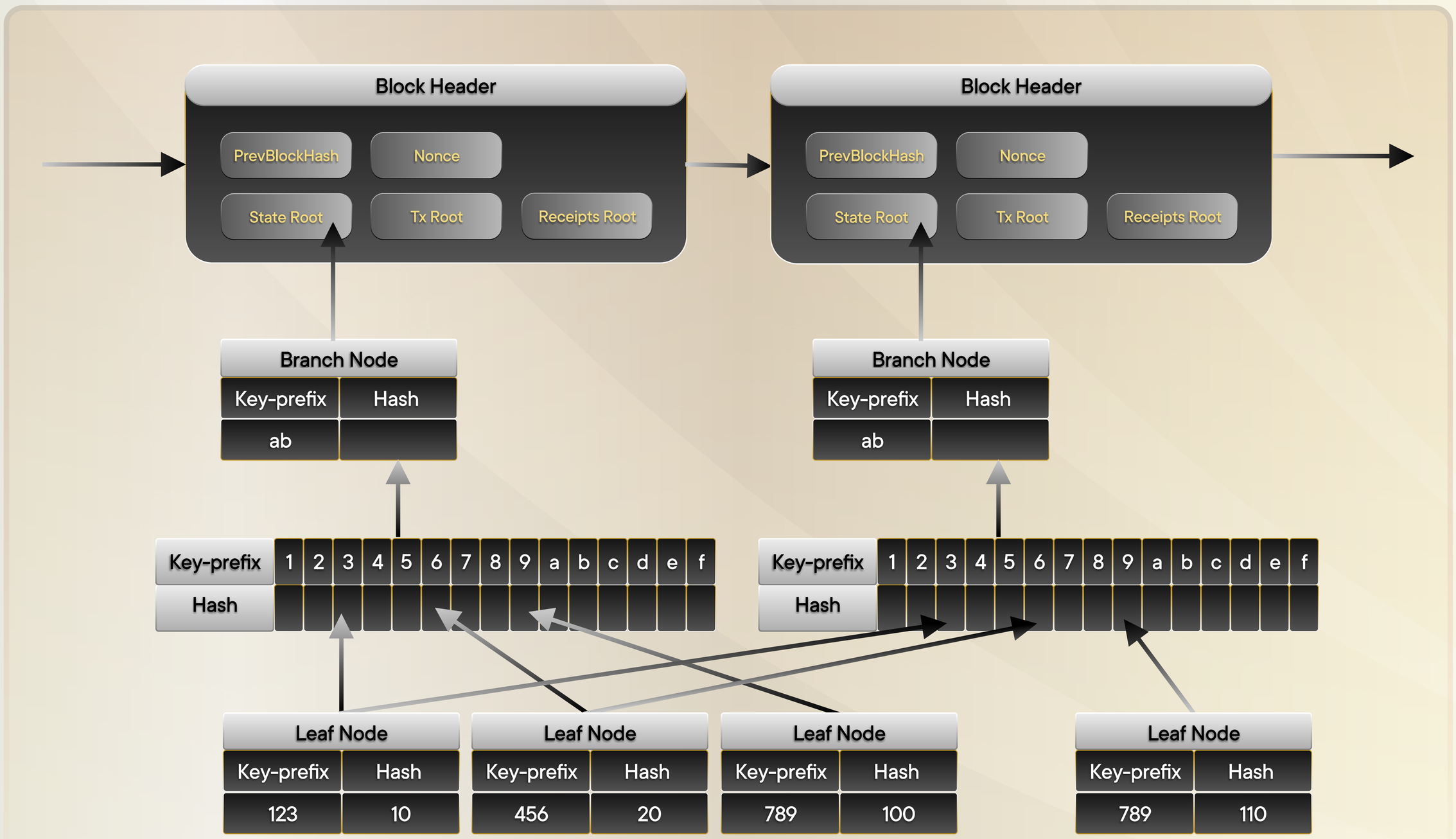

Fig. 10.2: MERKLE-PARCIA-TRIE STRUCTURE

10.3 Storage Sharding Technology

The BlackPearl.Chain public chain uses the Sharding technology to improve the throughput of the overall system through parallel consensus, block producing, and storage.

The storage strategy of the shards is designed as following:

In order to prevent double-spend problems, based on the from field, each transaction will be hashed to a specific shard. Each specific shard node stores only the state and transactions of some users.

As the data on the chain increase dramatically due to parallel computation, if each node in the shard needs to store the state and transactions of all users, storage will be a large burden, which will increase the access threshold of ordinary nodes. So, only the super storage node will store the full amount of data for all user state and transaction data.

10.4 Super storage nodes

Super storage nodes need to store transaction and user information for all shards. To prevent data loss after a storage node fails, the super storage node adopts the cluster deployment mechanism.

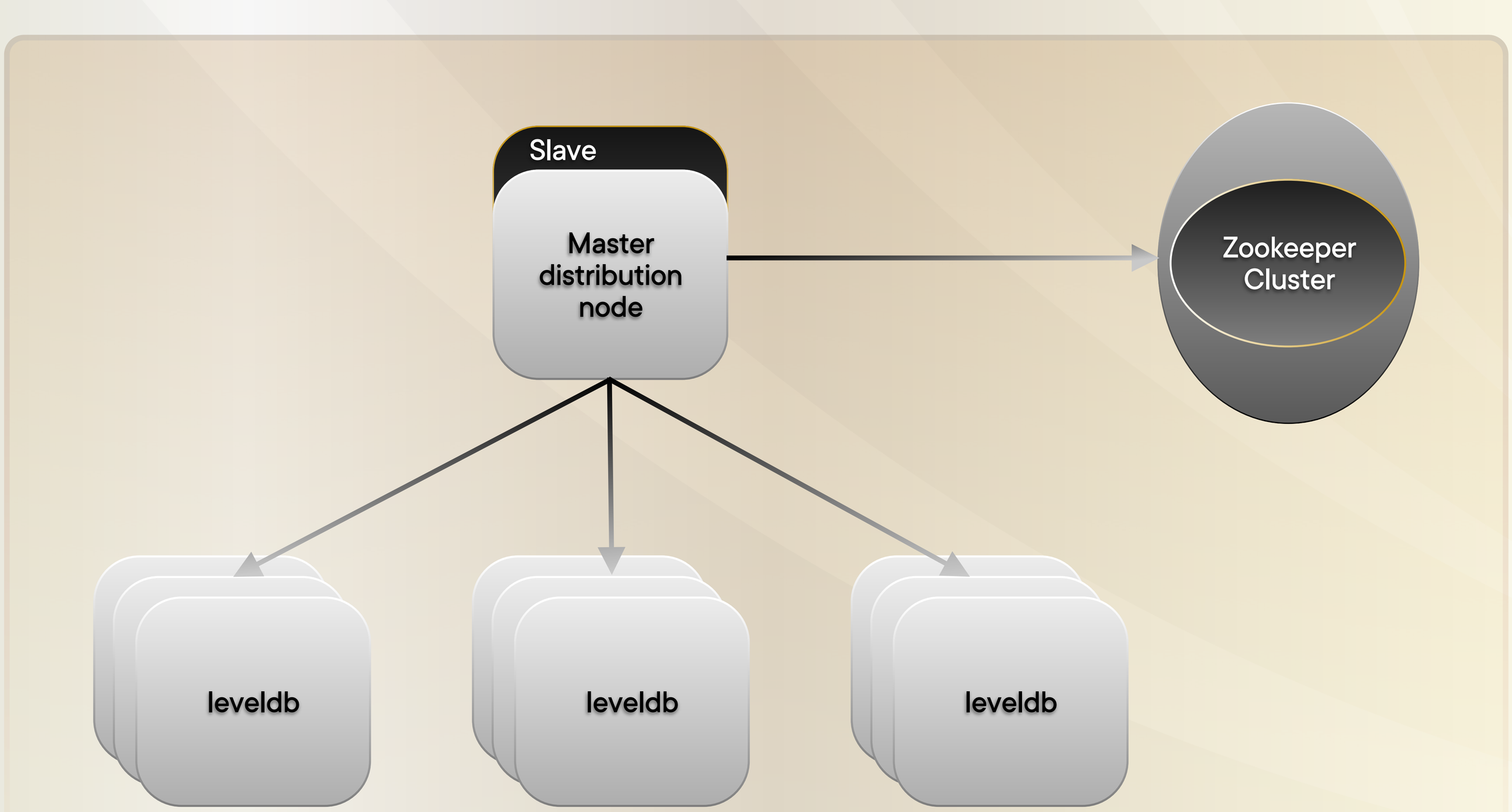

Fig. 10.3: SUPER STORAGE NODE

The master distribution node is responsible for scheduling the request and distributing specific requests to specific leveldb nodes. There is a backup for the master distribution node. When the master distribution node fails, the slave distribution node forwards the request.

Each leveldb small cluster stores the data corresponding to one shard. Use Zookeeper to select a main node from the leveldb cluster. There is also a copy node in the leveldb cluster. The copy node uses the commit log to keep the data synchronized with the main node. When the main node within leveldb fails, zookeeper selects the copy node which possess most updated data as the main node.

The Zookeeper cluster nodes guarantee consistency of configuration information through a distributed-consistent algorithm. The reliability of the global ledger is guaranteed by the high availability architecture of the super storage node as shown in Figure 10.3.

11. Incentive Model

The Sharding architecture design ensures an increase in system processing power as the parallel nodes increase. The public chain encourages nodes to increase online trading time and more participation in system transactions through incentives for active online trading nodes. The accounting node of each shard draws a 0.01% fee to the public chain foundation address when the fee is charged, and the funds on the account are used for random rewards to the online trading node.

Execution of transactions and smart contracts are subject to a handling fee (gas fee), and the user can set the gas value and maximum value for each transaction. At different stages of the transaction processing, different roles obtain a certain amount of gas fees. The revenue of the distribution center node and the super storage node is automatically generated by the blockchain, and it takes effect after the consensus recorded by the accounting node of each shard.

11.1 Accounting Node Reward

When the accounting node produces the block, the transaction handling fee (gas fee) is collected by accounting node. In general, a single transfer transaction handling fee (after deducting portion of it as collection node reward) is split evenly between the originator and the receiver. If the transaction fails to perform, the handling fee will be charged in full by accounting node. When executing a smart contract, if the contract execution fails, or fails to return within the set time, the accounting node collects the remaining handing fee. Each accounting node, when charging gas, draws 0.01% into the address of the public chain foundation address.

11.2 Collection Node Rewards

The collection node collects the transaction and package it, and sends it to the accounting node of each shard, and obtains the gas fee. The ratio of the gas fee reward is fixed. When the collection node integrates the transaction data, it calculates it's own income based on the gas fee, and adds a transaction record for self-increase. The accounting node of the shard verify the transactional data sent by the collection node, and check the correctness of the gas fee reward calculation, validate by consensus and write to the block for record.

11.3 Distribution Center Node Rewards

The distribution center obtains the reward according to the amount of To-be processed transaction. After the transaction sent by the collection node is validated, the shard node adds a transaction into the transaction package, which will increase the balance of the distribution center node according to the quantity of the transaction To-be processed and the built-in parameters of the public chain. Then, this transaction package will be sent to distribution center. After the consensus by shards, the transaction is confirmed, and the reward is validated.

11.4 Super storage Node Rewards

The super storage node stores the blockchain data and also provides transaction and contract inquiry services, the reward revenue of super storage node is based on the amount of stored data of the service provided. The accounting node on each shard adds a storage node balance increment transaction according to the amount of data (byte) synchronized to the super storage and the built-in parameters of the public chain. After the consensus, the transaction is confirmed, and the reward is validated.

11.5 User Online Foundation Random Rewards

The public chain uses a random reward for users, encouraging users to use the blockchain system for trading and running smart contract applications. According to a specific algorithm, when each transaction information is generated, the transaction information is also sampled at the same time, and a hash value is calculated. When the accounting node verifies the transaction, it compares the hash value with the hash value of the existing transaction address in the shard. When the two match, the transaction initiator obtains the online fund reward. The accounting node needs to add a smart contract call to enter the reward into the corresponding transaction address. After the smart contract is deployed on the public chain, it will be verified according to the set rules, and the transaction initiator who meets the requirements will perform a transfer transaction from the foundation address to the transaction initiation address to complete the reward distribution.

12. System upgrade with Trusted Computing

At present, Bitcoin and Ethereum have experienced some problems in the development process, such as the hard fork caused by the expansion of Bitcoin and the hard fork caused by the ETA hacking incident, in order to solve the blockchain upgrade difficult pain points, BlackPearl.Chain proposed a method of using trusted computing to achieve dynamic upgrades.

12.1 AI prediction

At present, Bitcoin and Ethereum have experienced some problems in the development process, such as the hard fork caused by the expansion of Bitcoin and the hard fork caused by the ETA hacking incident, in order to solve the blockchain upgrade difficult pain points, BlackPearl.Chain proposed a method of using trusted computing to achieve dynamic upgrades.

BlackPearl.Chain uses the combination of AI system and voting, because the system upgrade not only needs to take into account the interests of community members, but also needs to take care of the impact that the upgrade may have on the community. The upgraded AI system uses the impact of historical upgrades on the community (such as user size, community boom, etc.) to predict whether to upgrade is needed. As historical upgrade data becomes more abundant, the upgraded AI system will also become more intelligent. Fully handed over to AI may have some uncertainty, so community voting and AI are combined. AI and community voting each account for 50% of the upgrade.

12.2 Dual directory upgrade

Dual directory update method is adopted when updating the program. Every file that is running during background update is occupied and cannot be updated, thus, the old version is copied to another directory and then update the newly copied program file. At the same time, the md5 integrity check is performed on the new version. The boot process is equivalent to run a bootloader. The logic of the bootloader is to detect the version number and load the latest version of the application's process. Since the logic of bootloader is simple, almost no update requirement is needed for bootloader.

13. Account system

13.1 Account generation

The account system draws on the design of the Ethereum account system.

There are two types of accounts, user accounts and contract accounts. With the user account, you can send the transaction, trigger the contract code, all through private key. The contract account has an associated code that is triggered by the execution of the transaction or a message received from another contract.

The user account is defined by a pair of public and private keys. The specific process of generating an account is shown in Figure 13.1

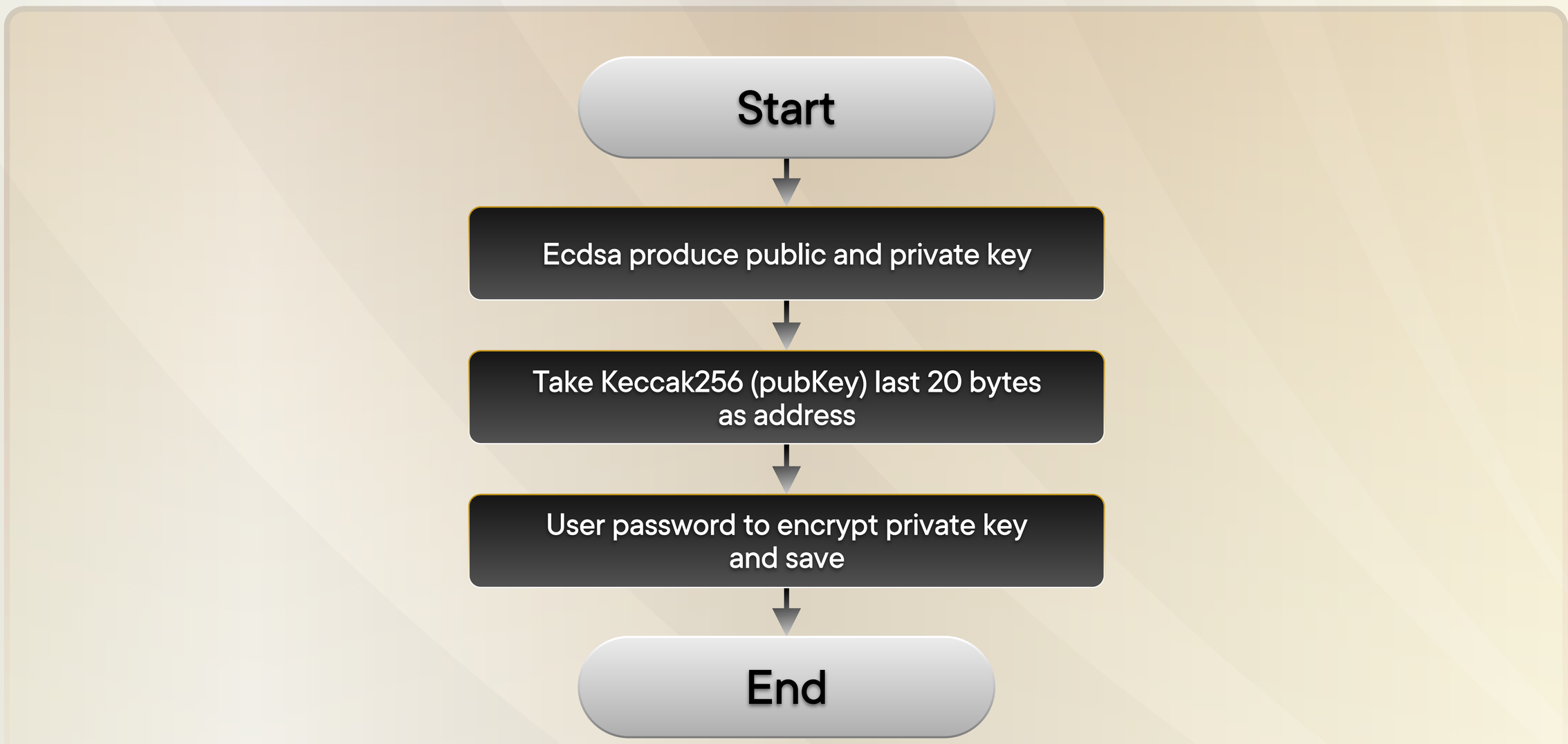

Fig. 13.1: ACCOUNT GENERATION PROCESS

The private key and the public key are first generated by an elliptic curve digital signature algorithm (curve of secp256k1). Then use Keccak256 to hash the public key and take the last 20 bytes as the account address. Finally, the private key is encrypted using the password entered by the user, and is stored in the keystore file along with the public key. The keystore is a readable json text file in which the private key is encrypted using password.

When account is generated, the account information will not be directly entered into stateRoot. This is to prevent hackers from attacking system by creating a large number of new accounts.

13.2 Support for account Import

Import the account by constructing a valid keystore file. The privateKey in the keystore file is unencrypted. When importing, you need to enter the password to encrypt the private key.

13.3 Recovery of private key

Once the private key is lost, it is equivalent to losing the password of the account, and all the coins in the account are lost.

The traditional solution is to back up the keystore and back up the password. This will restore the full public and private keys of the account.

Another way is to divide the user's private key into multiple copies, each of which is stored on a different machine. It also stores the XOR result for each copies. The rule based on the XOR operation:

For example, d = a^b^c

Then a = d^b^c

b = d^a^c

c = d^a^b

When one of the machines fails, it can be recovered by XORing the keys of several other machines

14. Smart Contract

14.1 Smart contract platform and compatibility

In order to provide high-performance blockchain services, BlackPearl.Chain had designed parallel execution and compatible smart contract platform. BlackPearl.Chain virtual machine architecture supports the operation of smart contracts and provides compatible support for existing public blockchain smart contract applications such as Ethereum and EOS.

Plan to use WebAssembley (WASM) for EOS, and Ethereum's smart contract can also be adapted to WASM (https//github.com/ewasm/design).

This will ensure more smart contract applications (DApp) quickly migrate to BlackPearl.Chain.

Smart Contracts can be used to build high-performance web applications and can be sandboxed with a small amount of adaptation.

14.2 Smart contract platform parallelism

When the smart contract is executed, the following three sub-processes need to be confirmed and verified:

a) internal consistency of the message;

b) all preconditions are valid;

c) Modify the application state.

The first two steps are read-only and can be executed in parallel. The final step to modify the application state requires that each application be processed in order.

The advantages of sharding improves the efficiency of parallel execution of smart contracts. Due to the use of sharding, the storage and execution of smart contract also need to find solution.

When the contract is deployed, the data is initially recorded on the local shard and synchronized to the super storage node to integrate the smart contract data of the entire network.

Here, BlackPearl.Chain need to solve the following problem.

How to quickly acquire and execute smart contracts from different shards?

In the entire network, only super storage nodes understand the full deployment of smart contracts. Due to the distributed storage of data, there is no way for individual shard node to directly obtain the contract information stored on other shards, the query service needs to be provided by the super storage node.

Considering the service capacity of the super storage node, the number of nodes and the TPS of the whole network, the design separates the communication between each shard node and the super storage node, reducing the performance pressure of a single storage node.

14.3 Recovery of private key

Inter-shard smart contract execution can lead to nested calls. How to ensure the correctness of the execution of the smart contract?

When a smart contract exists for nested calls, there may be cases where all the execution need to follow a certain order on multiple shard.

The accounting shard node that triggers the contract execution may need to complete the contract execution within a number of time slices and charge the gas fee.

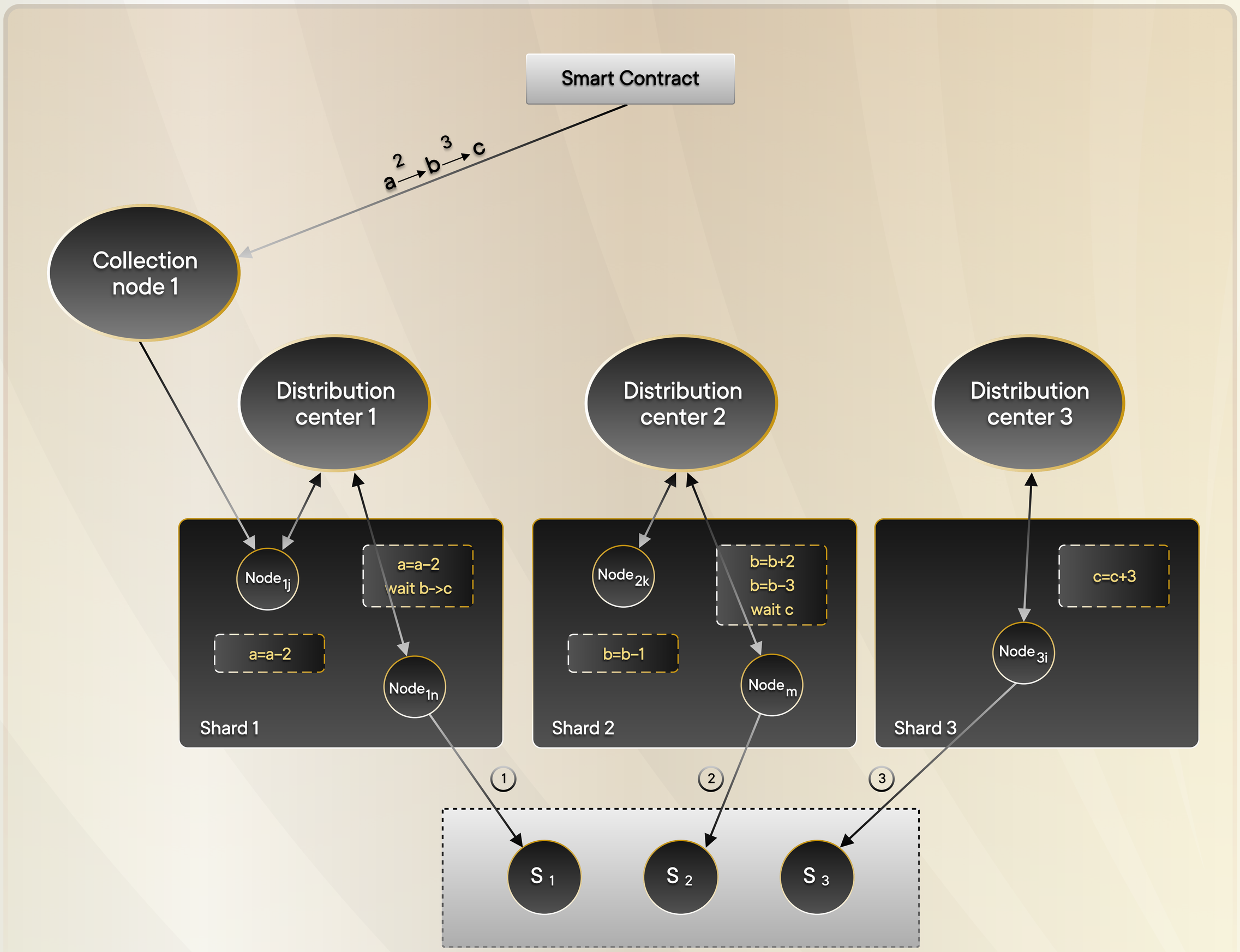

Fig. 14.1: SMART CONTRACT INTER-SHARD EXECUTION

However, since the execution of contract is performed across the shards, it is necessary to wait for the other shard to execute the code and produce the block before the triggering shard to record the result and enter it into the block. There is a sequence for data recording. The block producing is separated from the contract calling process. The last of the contract call is recorded in the block first. After the distribution center is updated, the pervious shard can then record the operation and enter it into block.

Also, in the same shard, the accounting node needs to synchronize and save the transaction and the state of the contract before recording result to the block.

If the execution of the contract fails, data needs to be rolled back. It is necessary to pay attention to the collection of the gas fee and the restoration of the state of each shard. The execution process is shown in Figure 14.1

15. Roadmap

2019 / Q2

Deployment of internal testing network: core module update, wallet user interface update, transaction pool optimization, consensus update, blockchain explorer update.

2019 / Q3

Deployment of testnet for public test: updates network sharding, transaction sharding, super routing, super storage node, smart contract platform. Ecosystem engagement: Users, developers.

2019 / Q4

Deployment of testnet with full features: state sharding, confirmation in seconds, millions TPS, System contract, anti quantum computation.

2020 / Q1

Mainnet lite deployment: public chain mapping, BNS neuron governance, DApp SDK, IPFS storage, linear expansion.

2020 / Q2

Mainnet deployment.

2020 / Q3 and beyond

BPL_Payment DApp, BPL_Message DApp, mainnet updates.

16. Token Model

Token Symbol: BPLC

Total supply of Token: 64,000,000,000 (Constant supply, volume will not change)

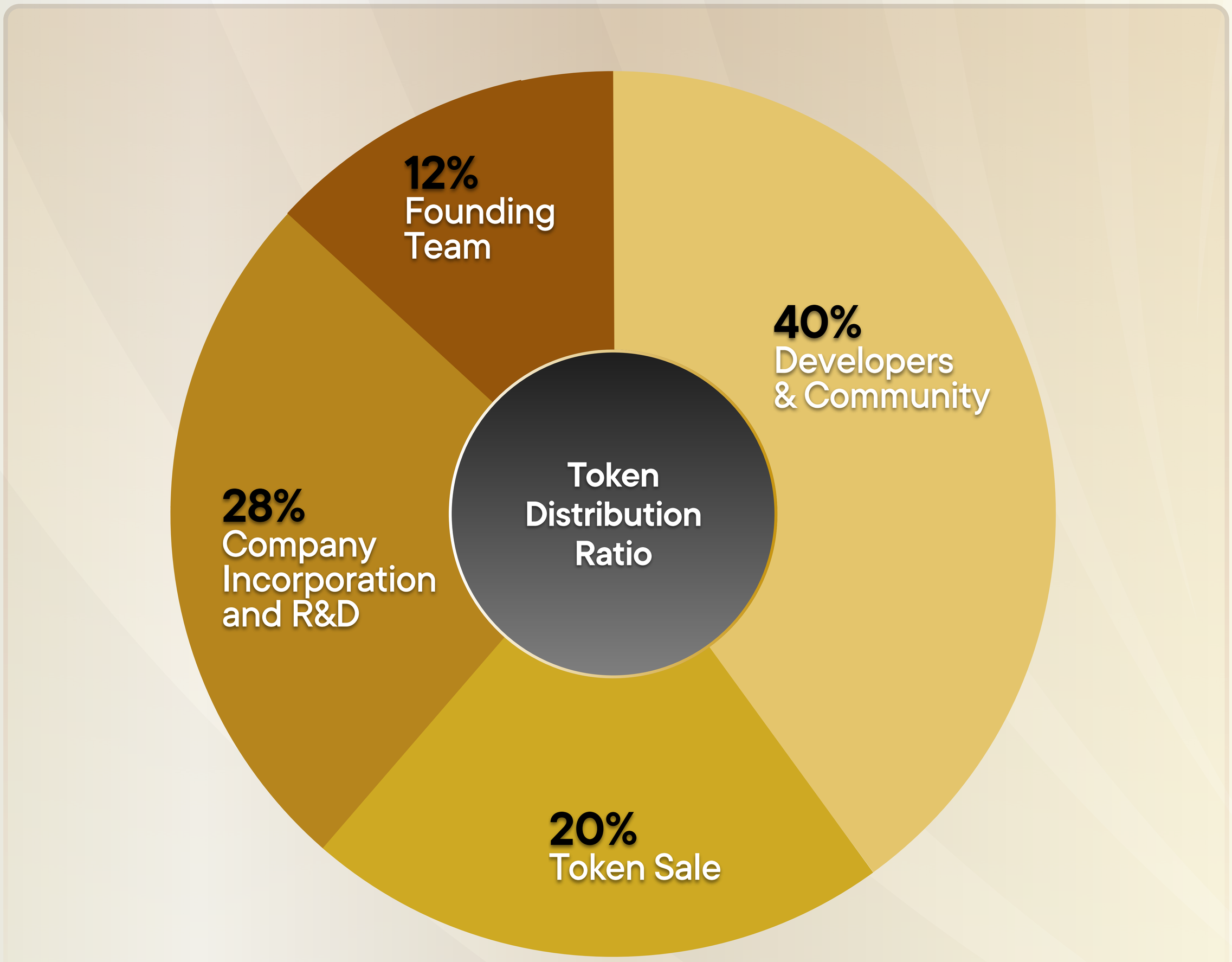

Fig. 16.1: TOKEN MODEL

The BPLC token is an infrastructural utility token with reduced volatility, initially based on ERC20 Ethereum standard. When mainnet is ready, the ERC20 token will be converted to BlackPearl.Chain native token. Initially, it will be used as a primary resource for funding project's R&D. Later, it is going to be used as a primary tool to power the BlackPearl.Chain platform. There are several different functions that will require the use of the BPLC totken. The DApp and smart contract execution, the user participation as node, the incentive rewards for BlackPearl.Chain platform ecosystem participants.

Token Sale Summary

This whitepaper explains the distribution of Tokens and the details of the Token Launch. It also briefly explains the purpose of a BlackPearl Token and its function within the BlackPearl Platform.

BlackPearl Platform will enables worldwide use (7B people) and 10T devices to run simultaneously, with millions TPS and seconds latency.

BlackPearl is an infrastructure with expandable throughput which can enable enterprise level decentralized applications. The BlackPearl Token is used on BlackPearl Platform to enable applications to pay gas fee in order to execute smart contract instruction. The Token is also used by the public chain software to give reward to BlackPearl network ecosystem participants such as Block producer node, super storage node automatically.

Use of Tokens

For the Token Launch, BlackPearl will issue the BPLC Token for public contribution. The Token has been classified as an Utility token based on its intended function.

The funding for development of BlackPearl Platform will be through a series of crowd sale. The initial funding of the BlackPearl Platform will be through a crowd sale offering 800,000,000 of the 12,800,000,000 initial Tokens. Tokens will be distributed in two crowd sales in period 1; (1) a private pre-sale; followed by (2) a public sale (From 5/23/2019 to 9/22/2019 at $0.075/BPLC). The 2nd period crowd sale will offer 4,000,000,000 initial Tokens (From 9/23/2019 to 12/22/2019 at $0.10/BPLC). The 3rd period crowd sale will offer 8,000,000,000 initial tokens (From 12/23/2019 to 6/22/2020 at $0.15/BPLC).

BPLC Token

The Token is an Ethereum based token implemented as ERC20 and is a Utility token that allows for participants to contribute and engage in building a blockchain ecosystem.

There will be 12,800,000,000 Tokens in existence after a series of crowd sales and no more Tokens will be issued for sale after the whole Token sale series are over. 12,800,000,000 Tokens for sale accounts for 20% of the whole Tokens supply, to ensure a wide distribution.

Token Sale Details

Token Symbol	BPLC
Private Pre-Sale	A round of private sale will take place before the Public Sale
Public Sale, period 1	6/23/2019 to 9/22/2019
Soft Cap	USD $500,000
Hard Cap	USD $60,000,000
Maximum available of Tokens generated	64,000,000,000 Tokens
Maximum available for purchase	800,000,000 Tokens (period 1)
Platform (Token type)	Ethereum (ERC20)
Accepted Currencies	ETH, BTC, Fiat
ETH/USD BTC/USD ratio	The price of ETH and BTC will be fixed at one day before starting of public sale The Token Launch completes either end of Public Sale or when the Hard Cap is reached.
Token Release Schedule	Tokens will be distributed starting from Public Sale date
USD Price per Token, period 1	USD $0.075

RISK FACTORS, DISCLOSURES, ACKNOWLEDGEMENTS AND WARRANTIES BY PURCHASERS AND OTHER NOTICES

IMPORTANT NOTICE: PROSPECTIVE PURCHASERS SHOULD CAREFULLY CONSIDER THE RISKS INVOLVED IN DETERMINING WHETHER PURCHASING THE TOKENS IS A SUITABLE INVESTMENT, CERTAIN OF WHICH ARE SUMMARISED BELOW.

In this section, unless the context otherwise requires, the risk factors and disclosures set out below shall also be deemed to apply in relation to BlackPearl Tokens as if references to Tokens were references to BlackPearl Tokens.

DISCLOSURES REGARDING TOKENS

Nature of Tokens

Except as explicitly set out in this whitepaper, Tokens do not have any rights, uses, purpose, attributes, functionalities or features, express or implied, including, without limitation, any uses, purpose, attributes, functionalities or features on the BlackPearl Platform. BlackPearl does not guarantee and is not representing in any way to a Purchaser that the Tokens have any rights, uses, purpose, attributes, functionalities or features. The purchase of Tokens does not provide a Purchaser with rights of any form with respect to BlackPearl or its revenues or assets, including, but not limited to, any voting, distribution, redemption, liquidation, proprietary (including all forms of intellectual property), or other financial or legal rights; is not a loan to BlackPearl; and does not provide the Purchaser with any ownership or other interest in BlackPearl.

Tokens are non-refundable

BlackPearl is not obliged to provide Purchasers with a refund for any reason and Purchasers will not receive money or other compensation in lieu of a refund. The Tokens are also not redeemable at the option of the Purchaser. Statements set out in this whitepaper are merely expressions of BlackPearl's objectives and desired work plan to achieve those objectives. and no promises of future performance or price are or will be made in respect to Tokens, including no promise of inherent value, and no guarantee that Tokens will hold any particular value.

Tokens are provided on an ‘as is’ basis

The Tokens are provided on an “as is” basis. The Associated Parties and each of their respective directors, officers, employees, shareholders, affiliates and licensors make no representations or warranties of any kind, whether express, implied, statutory or otherwise regarding the Tokens, including any warranty that the Tokens and the BlackPearl Platform will be uninterrupted, error-free or free of harmful components, secure or not otherwise lost or damaged. Except to the extent prohibited by applicable law, the Associated Parties and each of their respective directors, officers, employees, shareholders, affiliates and licensors disclaim all warranties, including any implied warranties of merchantability, satisfactory quality, fitness for a particular purpose, non-infringement, or quiet enjoyment, and any warranties arising out of any course of dealings, usage or trade.

Tokens may have no value

The Tokens may have no value and there is no guarantee or representation of liquidity for Tokens. BlackPearl is not and shall not be responsible for or liable for the market value of the Tokens, the transferability and/or liquidity of the Tokens and/or the availability of any market for Tokens through third parties or otherwise.

Lack of development of market of Tokens

There are no warranties that Tokens will be listed or made available for exchange for other cryptocurrency and/or fiat money. It shall be explicitly cautioned that if Tokens are made available on an exchange, such exchange, if any, may not be subject to regulatory oversight, and BlackPearl does not give any warranties in relation to any exchange services providers. Because there has been no prior public trading market for Tokens, the Token Launch may not result in an active or liquid market for Tokens, and the price of Tokens may be volatile. Token holders may not be able to dispose of Tokens easily and where no secondary market develops, a Token holder may not be able to liquidate at all. Proposed transfers of the Tokens may be blocked by BlackPearl in circumstances where the proposed transferee has not already completed BlackPearl’s KYC and AML procedures (including, without limitation, verification of identity and source of funds) to its satisfaction. Purchasers should be aware of the restrictions on their subsequent sale.

Risks relating to highly speculative prices

The valuation of cryptocurrency in a secondary market is usually not transparent, and highly speculative. The Tokens do not hold any ownership rights to BlackPearl's assets and, therefore, are not backed by any tangible asset. The value of Tokens in the secondary market, if any, may fluctuate greatly within a short period of time. There is a high risk that a Purchaser could lose its entire contribution amount. In the worst-case scenario, Tokens could be rendered worthless.

Force Majeure

The Token Launch and the performance of BlackPearl's activities set out in this whitepaper and the development roadmap may be interrupted, suspended or delayed due to force majeure circumstances. For the purposes of this whitepaper, "force majeure" shall mean extraordinary events and circumstances which could not be prevented by BlackPearl and shall include: changes in market forces or the technology, acts of nature, wars, armed conflicts, mass civil disorders, industrial actions, epidemics, lockouts, slowdowns, prolonged shortage or other failures of energy supplies or communication service, acts of municipal, state or federal governmental agencies, other circumstances beyond BlackPearl's control, which were not in existence at the time of Token Launch.

Insurance

Unlike bank accounts or accounts at financial institutions, Tokens are uninsured unless you specifically obtain private insurance to insure them. Thus, in the event of loss or loss of utility value, there is no public insurer or private insurance arranged by BlackPearl to offer recourse to a Purchaser.

GOVERNMENTAL DISCLOSURES

BlackPearl is not a regulated mutual fund

BlackPearl is not regulated as a mutual fund for the purposes of the Mutual Funds Law (2019 Revision) of the Cayman Islands ("MFL") on the basis that Tokens are not shares and BlackPearl is therefore not a registrable mutual fund. In addition, the Tokens are not redeemable at the option of

the Purchaser and so the Tokens and BlackPearl are considered 'closed-ended'. Accordingly, neither a copy of this whitepaper nor details about BlackPearl have been filed with the Cayman Islands Monetary Authority ("CIMA"). Because BlackPearl is not a regulated mutual fund, BlackPearl is not subject to the supervision of CIMA and BlackPearl is not required to have its accounts audited nor submit such accounts to CIMA.

If BlackPearl were regulated as a mutual fund under the MFL, it would need to comply with regulatory requirements designed to protect investors, including the requirement to limit the minimum aggregate Token purchase amount to US$100,000 or its equivalent in any other currency in order for it not to be licensed or administered by a licensed mutual fund administrator. BlackPearl would also need to pay a prescribed initial registration fee.

These are matters which would be required in connection with an initial registration under the MFL. BlackPearl would also then have ongoing obligations under the MFL following its initial registration, including the obligation to file with CIMA prescribed details of any changes to this whitepaper; to file annually with CIMA accounts audited by an approved auditor and a fund annual return; and to pay a prescribed annual fee.

If Company were a regulated mutual fund, it would also be subject to the supervision of CIMA, and CIMA would have wide powers to take certain actions if certain events occur.

Risk of unfavourable regulatory action in one or more jurisdictions

The regulatory status of cryptographic tokens, digital assets, and blockchain technology is undeveloped, varies significantly among jurisdictions and is subject to significant uncertainty. It is possible that certain jurisdictions may adopt laws, regulations, policies or rules directly or indirectly affecting the Bitcoin and Ethereum network, or restricting the right to acquire, own, hold, sell, convert, trade, or use Tokens. Developments in laws, regulations, policies or rules may alter the nature of the operation of the blockchain network upon which the Tokens are dependent. There can be no assurance that governmental authorities will not examine the operations of Associated Parties and/or pursue enforcement actions against Associated Parties. All of this may subject Associated Parties to judgments, settlements, fines or penalties, or cause Associated Parties to restructure their operations and activities or to cease offering certain products or services, all of which could harm Associated Parties' reputations or lead to higher operational costs, which may, in turn, have a material adverse effect on the Tokens and/or the development of the BlackPearl Platform.

Purchaser bears responsibility of legal categorization

There is a risk that Tokens might be considered a security in certain jurisdictions, or that they might be considered to be a security in the future. BlackPearl does not provide any warranty or guarantee as to whether the Tokens will be a security in the jurisdiction of the Purchaser. Each Purchaser will bear all consequences of Tokens being considered a security in their respective jurisdiction. Every Purchaser is responsible to confirm if the acquisition and/or disposal of Tokens is legal in its relevant jurisdiction, and each Purchaser undertakes not to use Tokens in any jurisdiction where doing so would be unlawful. If a Purchaser establishes that the purchase or use of Tokens is not legal in its jurisdiction (or would only be legal if the company had taken additional steps such as registration or licensing), it should not acquire Tokens and immediately stop using or possessing Tokens.

Acquiring Tokens in exchange for cryptocurrency will most likely continue to be scrutinised by various regulatory bodies around the world, which may impact the usage of Tokens. The legal ability of BlackPearl to provide or support Tokens in some jurisdictions may be eliminated by future regulation or legal actions. In the event that BlackPearl determines that the purchase or usage of Tokens is illegal in a certain jurisdiction, BlackPearl may cease operations in that jurisdiction, or adjust Tokens in a way to comply with applicable law.

Purchaser bears responsibility for complying with transfer restrictions

Tokens may be placed on third-party exchanges, giving future purchasers and users an opportunity to openly buy Tokens. A user seeking to enter the BlackPearl Platform following the Token Launch will have to buy Tokens on such exchanges. Conversely, Tokens may be sold on such exchanges if the holder of Tokens would like to exit the BlackPearl Platform ecosystem. Existing laws on the circulation of securities in certain countries, such as the United States of America, China, South Korea, Canada and Singapore, may prohibit the sale of the Tokens to the residents of those countries. When buying Tokens, Purchasers should be aware of the restrictions on their subsequent sale.

GENERAL SECURITY RISKS

Risk of theft and hacking

Token generation events and initial coin offerings are often targeted by hackers and bad actors. Hackers may attempt to interfere with the Purchaser's digital wallet, whether located on the BlackPearl Platform or otherwise, (the "Purchaser's Wallet"), the BlackPearl Smart Contract or the availability of Tokens in any number of ways, including without limitation denial of service attacks, Sybil attacks, spoofing, smurfing, malware attacks, or consensus-based attacks. Any such attack may result in theft of a Purchaser's Tokens.

Private keys

Tokens purchased by a Purchaser may be held by a Purchaser in the Purchaser's Wallet or vault, which requires a private key, or a combination of private keys, for access. Accordingly, loss of requisite private key(s) associated with Purchaser's Wallet or vault storing the Tokens will result in loss of such Tokens. Moreover, any third party that gains access to such private key(s), including by gaining access to login credentials of a hosted wallet or vault service Purchaser uses, may be able to misappropriate Purchaser's Tokens. BlackPearl is not responsible for and shall be held harmless in respect of any such losses.

Failure to map a public key to Purchaser's Wallet

Failure of the Purchaser to map a public key to such Purchaser's Wallet may result in third parties being unable to recognize buyer's Token balance on the Ethereum blockchain when and if they configure the initial balances of a new blockchain based upon the BlackPearl Platform.

Risk of incompatible wallet service

The wallet or wallet service provider used for the acquisition and storage of the Tokens has to be technically compatible with the Tokens. The failure to assure this may result in the Purchaser not being able to gain access to its Tokens.

Risk of weaknesses or exploitable breakthroughs in the field of cryptography

Advances in cryptography, or other technical advances such as the development of quantum computers, could present risks to cryptocurrencies, Ethereum and Tokens, which could result in the theft or loss of Tokens.

Internet transmission risks

There are risks associated with using Tokens including, but not limited to, the failure of hardware, software, and internet connections. BlackPearl shall not be responsible for any communication failures, disruptions, errors, distortions or delays you may experience when using the BlackPearl Platform and Tokens, howsoever caused. Transactions in cryptocurrency may be irreversible, and, accordingly, losses due to fraudulent or accidental transactions may not be recoverable. Cryptocurrency transactions are deemed to be made when recorded on a public ledger, which is not necessarily the date or time when the transaction is initiated.

BLACKPEARL PLATFORM DISCLOSURES

No guarantee that the BlackPearl Smart Contract will be developed

Each Purchaser acknowledges, understands and agrees that such Purchaser should not expect and there is no guarantee or representation or warranty by BlackPearl that:

- the BlackPearl Platform will ever be adopted;
- the BlackPearl Platform will be adopted as developed by BlackPearl and not in a different or modified form;
- a blockchain utilizing or adopting BlackPearl will ever be launched;
- BlackPearl Tokens will ever be made available or be exchangeable for Tokens; and
- a blockchain will ever be launched with or without changes to the BlackPearl Platform and with or without a distribution matching the fixed balance of Initial Tokens (as defined below).

Furthermore, the Tokens initially generated upon the Token Launch ("Initial Tokens") will not have any functionality or rights on the BlackPearl Platform and holding Initial Tokens is not a guarantee, representation or warranty that the holder will be able to use the BlackPearl Platform, or receive any tokens utilized on the BlackPearl Platform, even if the BlackPearl Platform is launched and the BlackPearl Smart Contract is adopted, of which there is no guarantee, representation or warranty made by BlackPearl.

Risks associated with the BlackPearl Smart Contract and associated software and/or infrastructure

The BlackPearl Smart Contract is based on the Ethereum blockchain. As such, any malfunction, unintended function or unexpected functioning of the Ethereum protocol may cause the Tokens and/or the BlackPearl Platform to malfunction or function in an unexpected or unintended manner.

The Ethereum blockchain rests on open source software, and accordingly there is the risk that the BlackPearl Smart Contract may contain intentional or unintentional bugs or weaknesses which may negatively affect Tokens or result in the loss or theft of Tokens or the loss of ability to access or control Tokens. In the event of such a software bug or weakness, there may be no remedy and Token holders are not guaranteed any remedy, refund or compensation.

On the Ethereum blockchain, timing of block production is determined by proof of work so block production can occur at random times. For example, Ether transferred to BlackPearl's recipient digital wallet address in the final seconds of a distribution period may not get included for that period.

Purchaser acknowledges and understands that the Ethereum blockchain may not include the Purchaser's transaction at the time the Purchaser expects and the Purchaser may not receive the Tokens the same day the Purchaser sends Ether, Bitcoin or fiat currency.

The Ethereum blockchain is prone to periodic congestion during which transactions can be delayed or lost. Individuals may also intentionally spam the Ethereum network in an attempt to gain an advantage in purchasing cryptographic tokens. The Purchaser acknowledges and understands that Ethereum block producers may not include the Purchaser's transaction when the Purchaser wants or the Purchaser's transaction may not be included at all.

Ether, the native unit of account of the Ethereum blockchain may itself lose value in ways similar to the Tokens, and also other ways. More information about Ethereum is available at http://www.ethereum.org.

Irreversible nature of blockchain transactions

Transactions involving Tokens that have been verified, and thus recorded as a block on the blockchain, generally cannot be undone. Even if the transaction turns out to have been in error, or due to theft of a user's Tokens, the transaction is not reversible. Further, at this time, there is no governmental, regulatory, investigative, or prosecutorial authority or mechanism through which to bring an action or complaint regarding missing or stolen cryptocurrencies and digital tokens. Consequently, BlackPearl may be unable to replace missing Tokens or seek reimbursement for any erroneous transfer or theft of Tokens.

Amendments to protocol

The development team and administrators of the source code for Ethereum blockchain or the BlackPearl Smart Contract could propose amendments to such network's protocols and software that, if accepted and authorized, or not accepted, by the network community, could adversely affect the supply, security, value, or market share of Tokens.

Risk of mining attacks

As with other decentralized cryptocurrencies, Ethereum blockchain, which is used for the Tokens, is susceptible to mining attacks, including but not limited to double-spend attacks, majority mining power attacks, "selfish-mining" attacks, and race condition attacks.

Any successful attacks present a risk to the Tokens, expected proper execution and sequencing of Tokens, and expected proper execution and sequencing of Ethereum contract computations in general. Despite the efforts of BlackPearl and Ethereum Foundation, the risk of known or novel mining attacks exists. Mining attacks, as described above, may also target other blockchain networks, with which the Tokens interact with and consequently the Tokens may be impacted also in that way to the extent described above.

Risk of default by player, athlete or club

The payment to a Purchaser of any monies, funds or tokens in connection with its holding of BlackPearl Tokens or Tokens is dependent upon the underlying player, athlete or club performing their obligations and ensuring that the monies, funds or tokens are available to the holders of

BlackPearl Tokens for distribution by the BlackPearl Smart Contract. There is a risk that the player, athlete or club defaults on their obligations and that the Purchaser never received any payments in connection with their holding of BlackPearl Tokens. These actions could adversely affect the BlackPearl Platform and the value and/or utility of any Token you own.

The holder of BlackPearl Tokens may have no contractual nexus or ability to instigate legal proceedings against the player, athlete or club where a default arises and should take specific legal advice on this matter before acquiring the Tokens or BlackPearl Tokens.

In addition, the player, athlete or club that a Purchaser has chosen to support by acquiring BlackPearl Tokens may never fulfil their potential, become successful or earn enough to generate a return for the Purchaser.

COMPANY DISCLOSURES

Legal structure of Token generator

BlackPearl is an exempted company incorporated in the Cayman Islands pursuant to the Companies Law (Revised) of the Cayman Islands. An exempted company is a body corporate which has separate legal personality capable of exercising all the functions of a natural person of full capacity irrespective of any question of corporate benefit, and having perpetual succession. The constitution of an exempted company is contained in two documents, the memorandum of association and the articles of association (the "**Articles**"). The Articles typically provide that there must be at least one director of a Cayman company. Generally, the Articles will specify that the management of a Cayman company is the responsibility of, and is carried out by, its board of directors. If the Articles permit it, a Cayman company may indemnify officers and directors of the company from all liabilities and expenses incurred by search persons in the performance of their duties.

The memorandum of association of a Cayman Islands company must specify the authorised share capital of such company. The memorandum of association will state the aggregate amount of the authorised share capital, together with details of the number of shares into which it is divided and the par value of those shares. As a Token holder, you are not a party to the memorandum of association or the Articles and are not entitled to any right or interest in or to shares of BlackPearl and have no rights to appoint or remove the board of directors of BlackPearl.

Because Tokens confer no governance rights of any kind with respect to the BlackPearl Platform or BlackPearl, all decisions involving BlackPearl's products or services within the BlackPearl Platform or BlackPearl itself will be made by BlackPearl at its sole discretion. These decisions could adversely affect the BlackPearl Platform and the value and/or utility of any Token you own.

Dependence on management team

The ability of the BlackPearl Platform project team which is responsible for maintaining competitive position of the BlackPearl Platform is dependent to a large degree on the services of a senior management team. The loss or diminution in the services of members of such senior management team or an inability to attract, retain and maintain additional senior management personnel could have a material adverse effect on the BlackPearl Platform and the value of the Tokens. Competition for personnel with relevant expertise is intense due to the small number of qualified individuals, and this competition may seriously affect BlackPearl's ability to retain its existing senior management and attract additional qualified senior management personnel, which could have a significant adverse impact on the BlackPearl Platform and the value of the Tokens.

Risks related to reliance on third parties

Even if completed, the BlackPearl Platform will rely, in whole or in part, on third-parties to adopt and implement it and to continue to develop, supply, and otherwise support it. There is no assurance or guarantee that those third-parties will complete their work, properly carry out their obligations, or otherwise meet anyone's needs, any of which might have a material adverse effect on the BlackPearl Platform and the value of the Tokens.

Insufficient interest in the BlackPearl Platform and the Tokens

It is possible that the BlackPearl Platform or Tokens will not be used by a large number of individuals, businesses and organizations and that there will be limited public interest in the creation and development of its functionalities. Such a lack of interest could impact the development of the BlackPearl Platform and the value of the Tokens.

BlackPearl Platform development risks

The development of the BlackPearl Platform and/or BlackPearl Smart Contract may be abandoned for a number of reasons, including lack of interest from the public, lack of funding, lack of commercial success or prospects, or departure of key personnel.

Changes to the BlackPearl Platform

The BlackPearl Platform is still under development and may undergo significant changes over time. Although Associated Parties intend for the BlackPearl Platform to have the features and specifications set forth in this whitepaper, changes to such features and specifications may be made for any number of reasons, any of which may mean that the BlackPearl Platform does not meet the expectations of the Purchaser.

Other projects

The BlackPearl Platform may give rise to other, alternative projects, promoted by parties that are affiliated or unaffiliated with the Associated Parties, and such projects may provide no benefit to the BlackPearl Platform.

Disclosures relating to conflicts of interest

Any of the Associated Parties may be engaged in transactions with related parties and conflicts of interest may arise, potentially resulting in the conclusion of transactions on terms not determined by market forces.

ACKNOWLEDGEMENTS AND WARRANTIES BY PURCHASERS

Acknowledgements

By (i) accessing or accepting possession of any information in this whitepaper (or any part thereof) or (ii) transferring payment (whether in fiat currency or cryptocurrency) and agreeing to purchase the Tokens, each Purchaser agrees and acknowledges that:

- the Tokens do not and are not intended to constitute securities in any jurisdiction. This whitepaper does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities or a solicitation for investment in securities in any jurisdiction;
- the Tokens are meant for internal use within the BlackPearl Platform and are not intended as securities or other assets to be used for speculative trading purposes. BlackPearl does not operate an exchange for Tokens and there is no guarantee of the future value of the Tokens. BlackPearl does not take any responsibility for any trade in Tokens in or through third-party exchanges. The possibility exists that the Tokens could be worth nothing;
- this whitepaper does not constitute or form part of any opinion on, any advice to buy or sell, or any solicitation of any offer to purchase any Tokens nor shall it or any part of it nor the fact of its presentation form the basis of, or be relied upon in connection with, any contract or any investment or purchase decision;
- no regulatory authority in any applicable jurisdiction has examined or approved of the information set out in this whitepaper and the publication, distribution or dissemination of the whitepaper to you does not imply that any applicable laws, regulatory requirements or rules have been complied with;
- any agreement as between BlackPearl and a Purchaser, and in relation to any sale and purchase, of Tokens is, in the absence of Purchase Documents, to be governed by this whitepaper;
- notwithstanding any other section of this whitepaper, and to the extent permissible by applicable laws, BlackPearl shall not be liable for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including but not limited to loss of revenue, income or profits, and loss of use or data), arising out of or in connection with any acceptance of or reliance on this whitepaper or any part thereof by a Purchaser;
- no information in the whitepaper should be considered to be business, legal, financial or tax advice regarding BlackPearl, the Tokens or the Token Launch; and
- they should consult their own legal, financial, tax or other professional adviser regarding BlackPearl and its respective businesses and operations, the Tokens and the Token Launch.

ACKNOWLEDGEMENTS AND WARRANTIES BY PURCHASERS

Warranties

By (i) accessing or accepting possession of any information in this whitepaper (or any part thereof) or (ii) transferring payment (whether in fiat currency or cryptocurrency) and agreeing to purchase the Tokens, each Purchaser represents and warrants to BlackPearl as follows:

- that they have read, understood and accepted sole responsibility for the disclosed and undisclosed risks, disclaimers and other disclosures inherent in participating in the Token Launch and the purchasing of Tokens as set out in this whitepaper;
- that they are not a citizen or resident of any jurisdiction or territory into which a sale or distribution of the Token would be unlawful (each a “Prohibited Territory”) and are not purchasing the Tokens on behalf of, whether directly or indirectly, a citizen of any Prohibited Territory;
- that they have the power to enter into, exercise any rights and perform and comply with their obligations under this whitepaper and their entry into, exercise of their rights and/or performance of or compliance with their obligations under this whitepaper including accessing, distribution or dissemination of this whitepaper, is not prohibited or restricted by the applicable laws, regulations or rules in the Purchaser’s jurisdiction or country of residence, and where any restrictions in relation to the aforementioned are applicable, the Purchaser:
- accepts sole liability for non-compliance with such applicable laws, regulations and rules in the Purchaser’s jurisdiction or country of residence; and
- has observed and complied with all such applicable laws, regulations and rules in the Purchaser’s jurisdiction or country of residence at the Purchaser’s own and sole expense;
- that all actions, conditions and things required to be taken, fulfilled and done:
- in order to enable the Purchaser to lawfully enter into, exercise their rights and perform and comply with their obligations imposed by this whitepaper and to ensure that those obligations are legally binding and enforceable; and
- for the issue of the Tokens on the terms and conditions set out in this whitepaper, have been taken, fulfilled and done;
- that all the Purchaser’s obligations under this whitepaper are valid, binding and enforceable on such Purchaser in accordance with their terms;
- that the Purchaser has adequate understanding of the operation, functionality, usage, storage, transmission mechanisms and other material characteristics of cryptocurrencies, blockchain-based systems, cryptocurrency wallets or other related coin/token storage mechanisms, blockchain technology and smart contract technology;

- that the Purchaser is not exchanging cryptocurrencies for Tokens for the purpose of speculative investment or for the purpose of exchanging one form of virtual currency for another, with the present intention of delivering the Tokens to another person, in a coordinated series of steps intended to complete a single transaction;
- that the Purchaser is acquiring Tokens primarily for use in the BlackPearl Platform; and
- all of the above representations and warranties are true, complete, accurate and non-misleading from the time of the Purchaser's pre-registration (where applicable) and purchase of Tokens pursuant to the Token Launch.

OTHER NOTICES

AML and KYC

Measures aimed at the prevention of money laundering and terrorist financing will require a Purchaser to verify their identity and/or the source of funds to BlackPearl. This procedure may apply on all or any of (i) the initial purchase of the Tokens, (ii) the use of the BlackPearl Platform, (iii) the exchange of the Tokens for BlackPearl Tokens, (4) the transfer of the Tokens, (5) the receipt of any BlackPearl Tokens via the BlackPearl Smart Contract or (vi) as BlackPearl deems necessary or desirable in connection with its AML and KYC policies and procedures.

By way of example, an individual may be required to produce the original passport or identification card or copy duly certified by a public authority such as a notary public, the police or the ambassador in his country of residence, together with two original documents evidencing his address such as a utility bill or bank statement or duly certified copies. In the case of corporate applicants this may require production of a certified copy of the Certificate of Incorporation (and any change of name) and of the Memorandum and Articles of Association (or equivalent), and of the names and residential and business addresses of all directors and beneficial owners.

The details given above are by way of example only and BlackPearl will request such information and documentation as it considers is necessary to verify the identity and source of funds of a prospective Purchaser.

Each Purchaser acknowledges that BlackPearl shall be held harmless against any loss arising as a result of a failure to provide such information and documentation as has been requested by BlackPearl.

Each Purchaser further acknowledges and agrees that any failure by them to comply with BlackPearl's requests in relation to measures aimed at the prevention of money laundering and terrorist financing, may result in action being taken against the Purchaser in respect of the Tokens including, without limitation, the suspension or withdrawal of the Purchaser's account on the BlackPearl Platform or the Tokens held by them.

18. References

[1] Honey badger BFT protocol:
https://eprint.iacr.org/2016/199.pdf

[2] Ethash-PoW:
https://github.com/ethereum/wiki/wiki/Ethash

[3] Merkle patricia tree:
https://github.com/ethereumjs/merkle-patricia-tree
or:
https://github.com/ethereum/wiki/wiki/Patricia-Tree