PIRI BLOCK CHAIN

Whitepaper

https://pirichain.com

V.1.0.2

July 2022, Konya

CONTENTS

DEFINITIONS & ABBREVIATIONS

- SQL: Structured Query Language
- dPoS (Delegated proof of stake) : Delegate-based proof-of-stake algorithm
- FIFO (First In First Out): First in processing first-in, first-out approach.
- BaaS: Blockchain as a service.

WHAT IS PIRICHAIN?

Piri Blockchain, or Pirichain, is built on a delegation-based proof-of-stake consensus algorithm (dPoS). In Pirichain, different methods are also included rather than the classical methods used in blockchains. As its name is known, it was inspired by the famous Turkish traveler, Sailor Piri Reis.

Pirichain's biggest innovations besides the standard transactions available on blockchains; adding special data into transactions and creating smart scenarios based on addresses.

Pirichain Smart Scenario System consists of address infrastructure, not token infrastructure like Ethereum's Smart Contracts. Thus, the addresses of smart scenarios are directly individuals or institutions. In the address-based system, it is not possible to engage in undesirable situations such as forgery/fraud. Smart scenarios, such as SQL language; It has the roles of querying the information in the block network, making transactions, running a trigger or sending data / assets to another smart scenario. Thus, in addition to being fully compatible with the Web 3.0 concept, it also provides an infrastructure to create an information ecosystem built on blockchain technology, which is very rare in the world.

Pirichain was prepared and published as a master's thesis under the Department of Computer Engineering at Konya Technical University (August 2022). Its application was developed in parallel with the thesis.

Our upcoming projects are as follows.

- Stock Market Studies, where only PIRI will be the parity,
- Implementation of documents, payment and data structures by creating a multi-chain network special for companies (especially the Finance-Bank sector),
- Establishment of stable coin (USDT, USDC, etc.) bridge infrastructure,
- Standardization and customization of data structures and scenarios specific to Supply Chain, Law, Pharmaceuticals, Medicine, Economics (Banking-Finance) and other sectors,
- Making Pirichain a unique information ecosystem platform on the blockchain roof all over the world.

Our aim will not be limited to crypto systems service only. Our most important aim is to represent the building blocks of the cutting-edge technological concept that will be adopted in the near future as BaaS (Blockchain as a Service).

1. PIRICHAIN INFRASTRUCTURE

As seen in the system in Figure 1.1, end users and companies send requests to the server side. The system first puts it in a queue, the processing queue processes the incoming request and sends it to the nodes. After processing by the nodes, the result is sent back to the servers. In these transactions, each request and registration transaction is queued by queuing (FIFO).

Each block generation period is 10 seconds. And a result related to that transaction is expected from the node within a maximum of 30 seconds. When we test it practically; It takes approximately 150-400 milliseconds for a transaction to be sent from the server to the nodes and returned to the server side. In case of too much traffic in the system, different results are obtained depending on the hardware configuration of the node and internet speed.

OS	CPU	Memory	Network	Avg. Response Time
Windows 10	2	4	~ 10mbps	~ 8000 ms
Ubuntu 20.4	1	2	~ 10mbps	~ 5200 ms

1.1. Pirichain specific block fields

Validators: is an array type field stored in the Piri blockchain. When the block approval is received by the nodes, the information in this field is added.

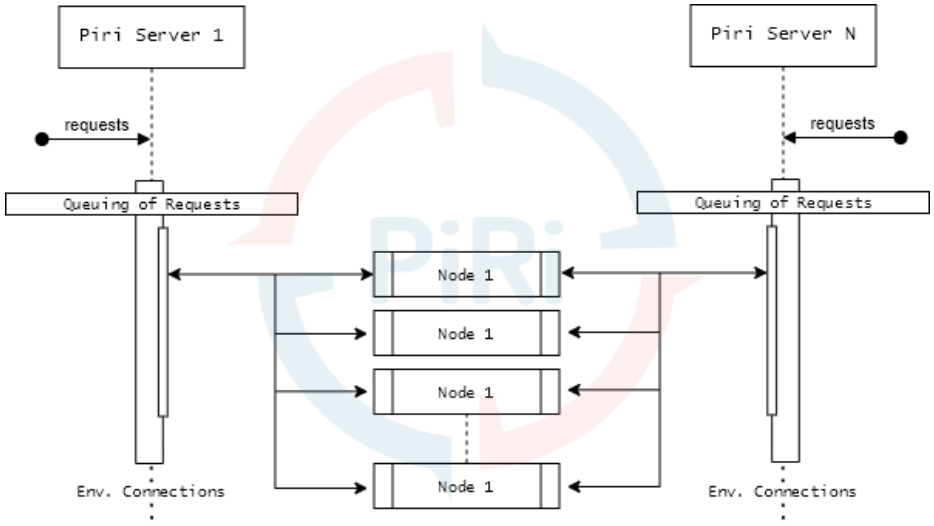


Figure 1.1: Relationship Between Pirichain Server and Nodes

1.2. Pirichain-specific transaction fields

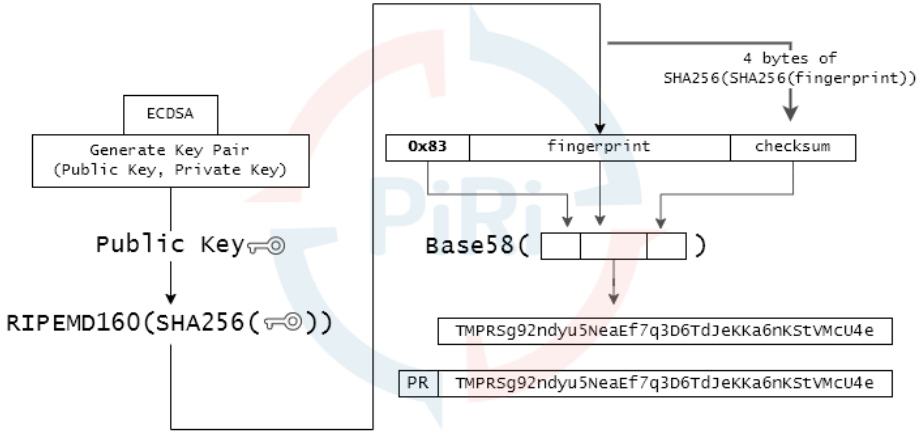
ValidatorNodes[]: The confirmation of the transaction, which is confirmed and recorded by the nodes in the Piri blockchain, is displayed in this area. The field is of array type.

Asset ID: There are not only PIRI assets in the Piri blockchain. It also has a token creation feature. Whether the transaction is a PIRI transfer or a Token transfer can be understood by looking at this area.

1.3. Pirichain Wallet Structure

Pirichain generates a private address (public key) and private key (private key) for each user. This address method is based on Elliptic Curve Asymmetric Encryption (ECDSA), a set of RIPEMD160 and SHA256 algorithms. The flow chart is shown in Figure 1.2.

Another important value in the wallet is the private key. In case of loss of private key, all asset(s) in the account will be lost. And it is not possible to add new information belonging to that address. In Pirichain, the private key is translated to 24 phrases via BIP39 (Walker, 2020) word deterministic translation module. The Pirichain system allows phrases to be created in 7 different languages (Chinese, Japanese, Korean, French, German, Spanish, Portuguese). This forces mnemonic words to be saved in an external location



.**Figure 1.2:** Wallet creation flowchart on Pirichain

Pirichain As seen in the BIP39 flowchart in Figure 1.3, the randomly generated entropy (randomness collected by an operating system) is found and the process continues (Walker, 2020).

In Pirichain, all assets are kept in the wallet. At the same time, the address to send data to the block is also part of the wallet. In fact, for the user, it can also be called the identity number of his/her wallet. There are 2 different types of wallet creation, Personal Wallet and Business Wallet.

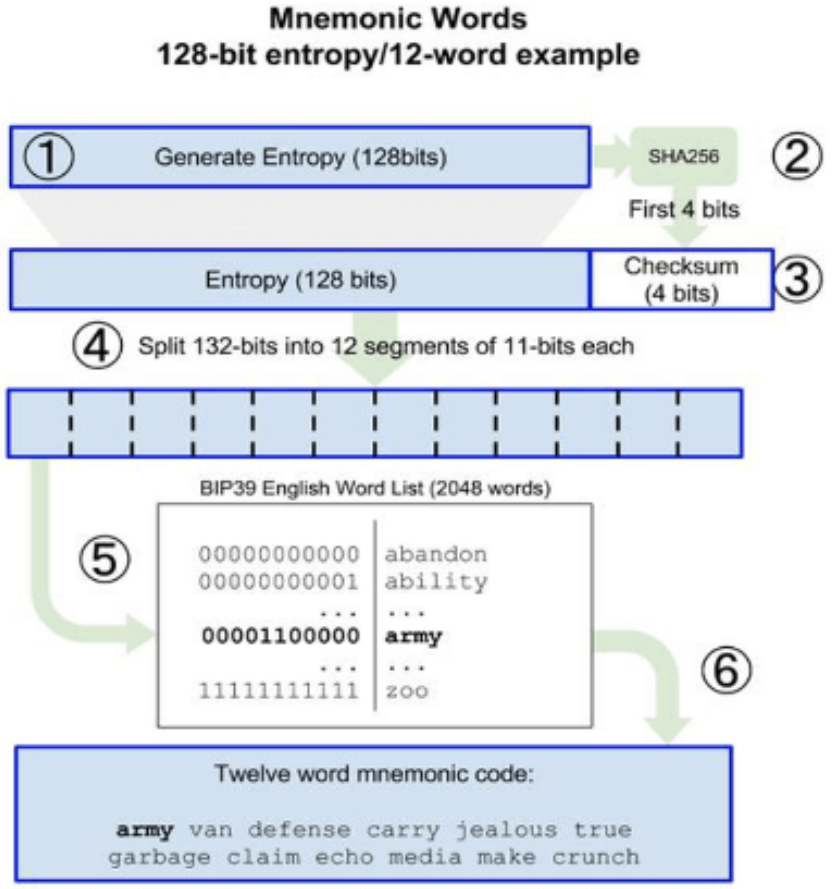


Figure 1.3: Word generation flowchart.

Personal Wallet: Personal wallets are types of wallets that do not have a commercial purpose. It is generally preferred by end users. These wallets have features for transferring Piri Coin between exchanges or adding data to the blockchain.

Business Wallets: There are 2 biggest differences from personal wallets. First; They can only send Piri Coin or other assets to commercial wallets, secondly, they cannot send Piri Coins to private wallets or exchanges outside Pirichain. In order to protect commercial wallet holders, Piri Coin will be bought directly from Pirichain company at a cheaper and fixed price. The main action of commercial wallets should be to add data to the block. They will be able to have Piri Coin much cheaper than the market.

1.4. Creation of Pirichain Transaction

The transaction record created in Pirichain is shown in the flow diagram in Figure 1.5.

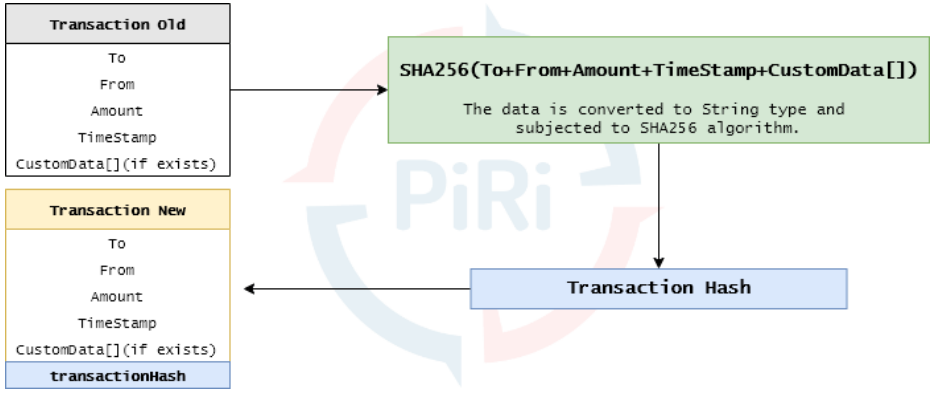


Figure 1.4: Creating the Transaction.

To give the summary value of the relevant transaction as shown in Figure 1.4; The above fields are subjected to the SHA256 algorithm and the identity information of that transaction record is created. The most important property here is the timestamp. Repetition is impossible in timestamps, although other fields are repeatable. The CustomData[] field is optional.

Figure 1.5 shows the post-data exchange operations between the server and the node.

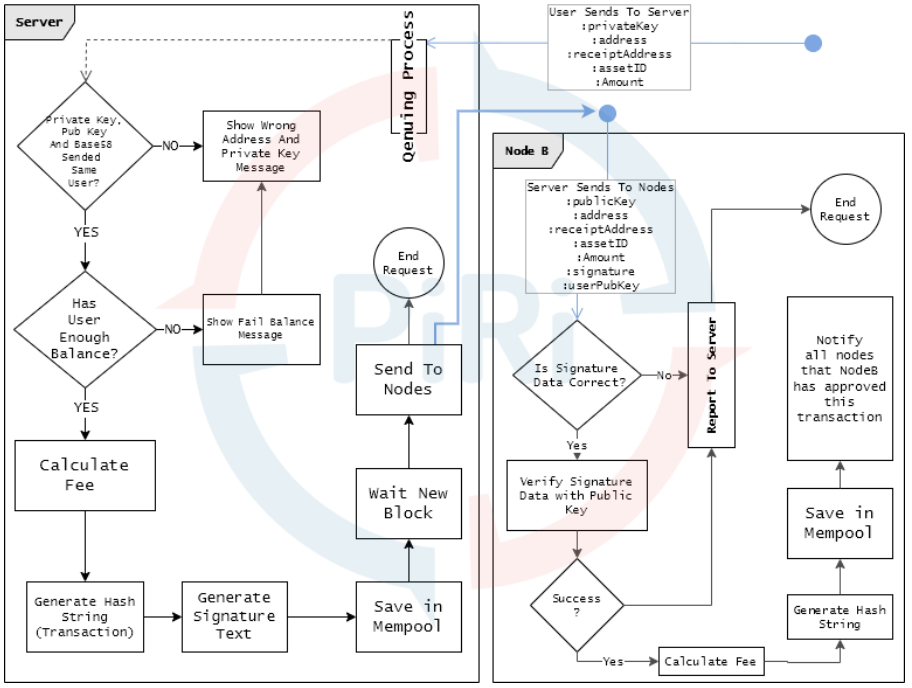


Figure 1.5: Data flow diagram between server-node

The relationship between node-node is shown in Figure 1.6. As can be seen, the system; It both wants to verify all transactions from the servers and also requests the result of the transaction record sent to all nodes.

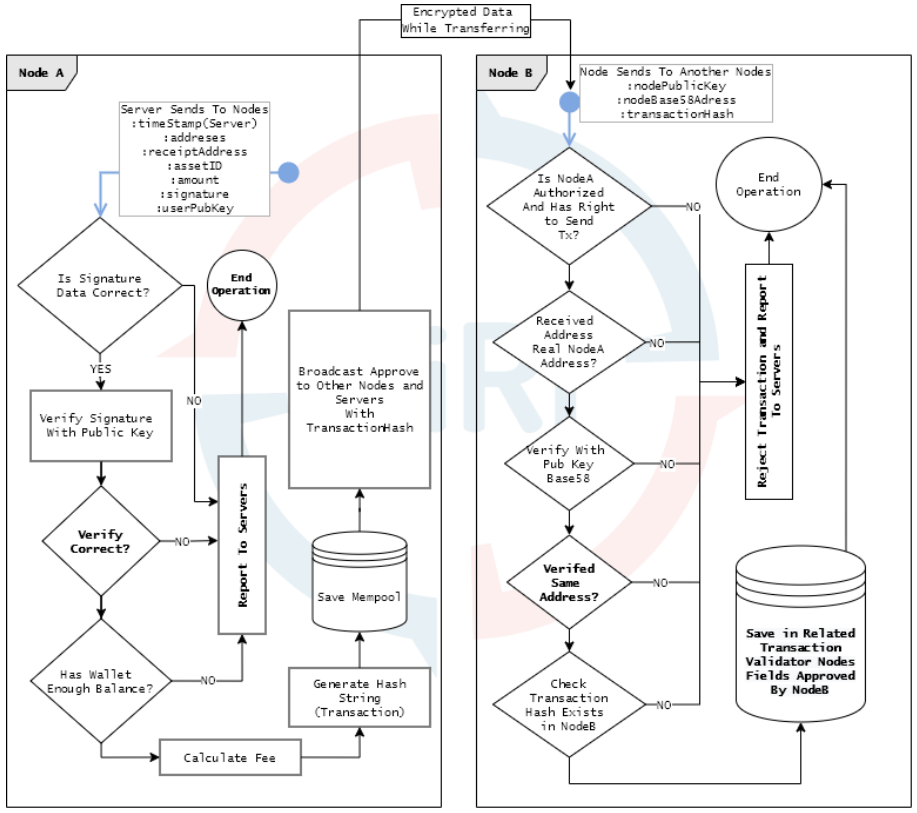


Figure 1.6: Control and data flow diagram between node and node

1.5. A New Concept in Blockchains! Adding Data to the Blockchain

Generally used areas in today's blockchains are crypto assets. But limiting it only in this area does not reflect the true power of blockchains. The platform-independent presence of the user in blockchains is one of the most important components of this technology. Figure 1.8 describes the data processing and authorization control flow diagram in Piri Blockchain.

As seen in Figure 1.7, there are 2 different encryption options.

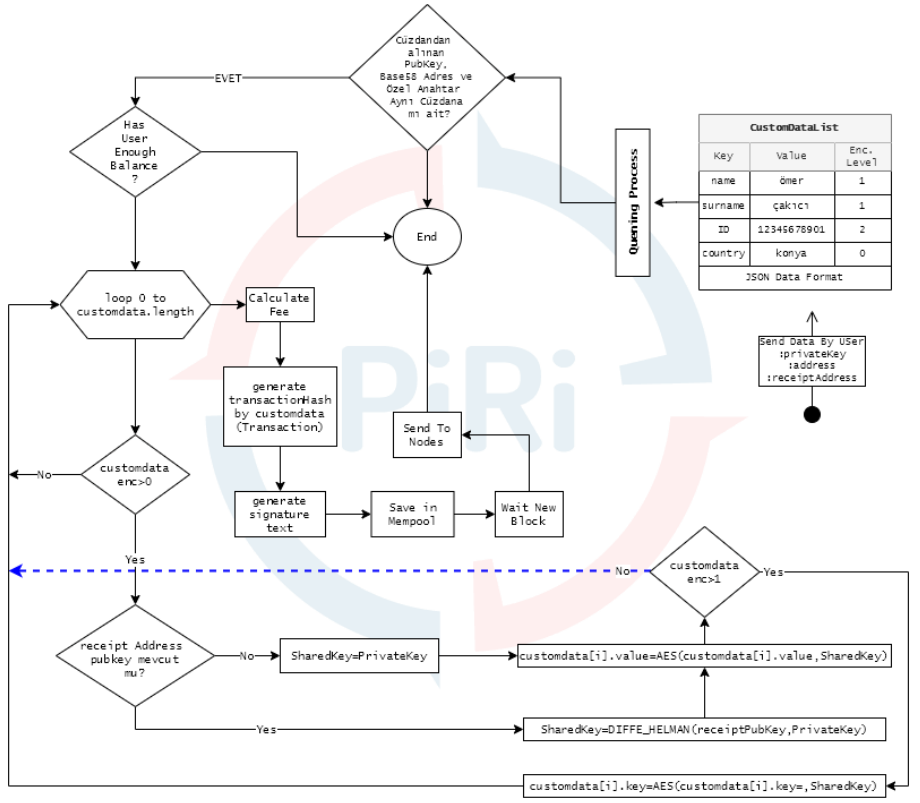


Figure 1.7: Diagram of private data storage and encryption

The first level (enc=1) is only encryption of data. In other words, it is the encryption of only the value field from the Key-Value pair. The second level is the encryption of both the "Key" and the "Value". The user can decide for himself/herself which level to encrypt.

Another situation is that the opposite address (Receipt Address) is a commercial wallet, in which case the public key of the commercial address is stored in Pirichain. Thus, when the data is desired to be decoded, this information can be easily retrieved by the system. It is not possible for

private wallets to generate a shared key with a receipt address. They can only add data to the block network by encrypting it with their private key. Therefore, data encrypted by private wallets can only be decrypted by that wallet. In commercial wallets, the shared key created by ECDSA Diffe Helman is used. Since this shared key creates the same value on both its side and the other side, the data can be decrypted on both sides. Detailed explanation for data analysis processes in the system is shown in Figure 1.8.

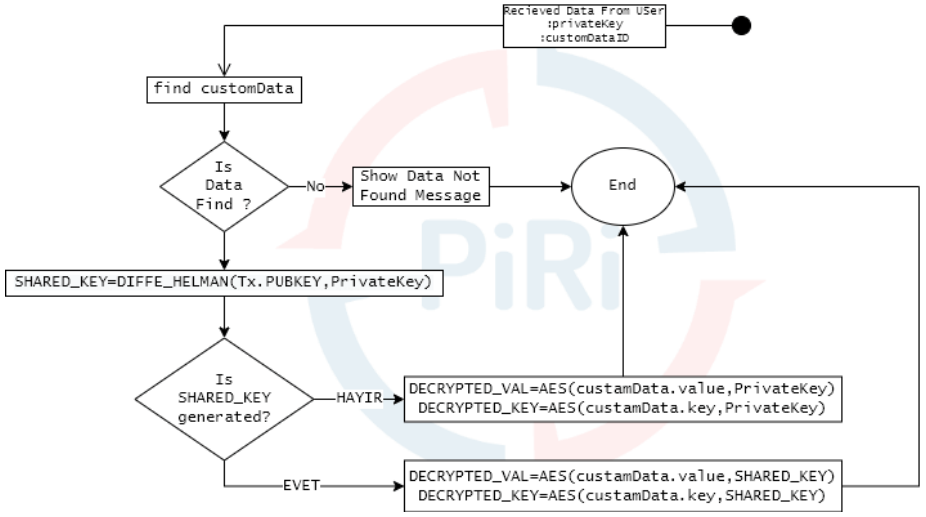


Figure 1.8: Data analysis operations

As seen in Figure 1.8, SHARED_KEY, which is determined as the public key in the analysis operations, is subjected to AES while generating. If there is a problem in the creation, decryption is tried over AES with the user's private key.

1.6. Pirichain's Web Server Services Structure

The diagram describing the relationship between Pirichain database and services is shown in Figure 1.9. In the system, every transaction is handled primarily via WEB API or WS (Web Socket) API. Connecting to these end points is done with SSL (Secure Socket Layer). The resulting request is evaluated by the modules and transferred to the services. In services, it becomes final or rejected. Services have permission to connect directly to databases. Modules only carry information to services or endpoints.

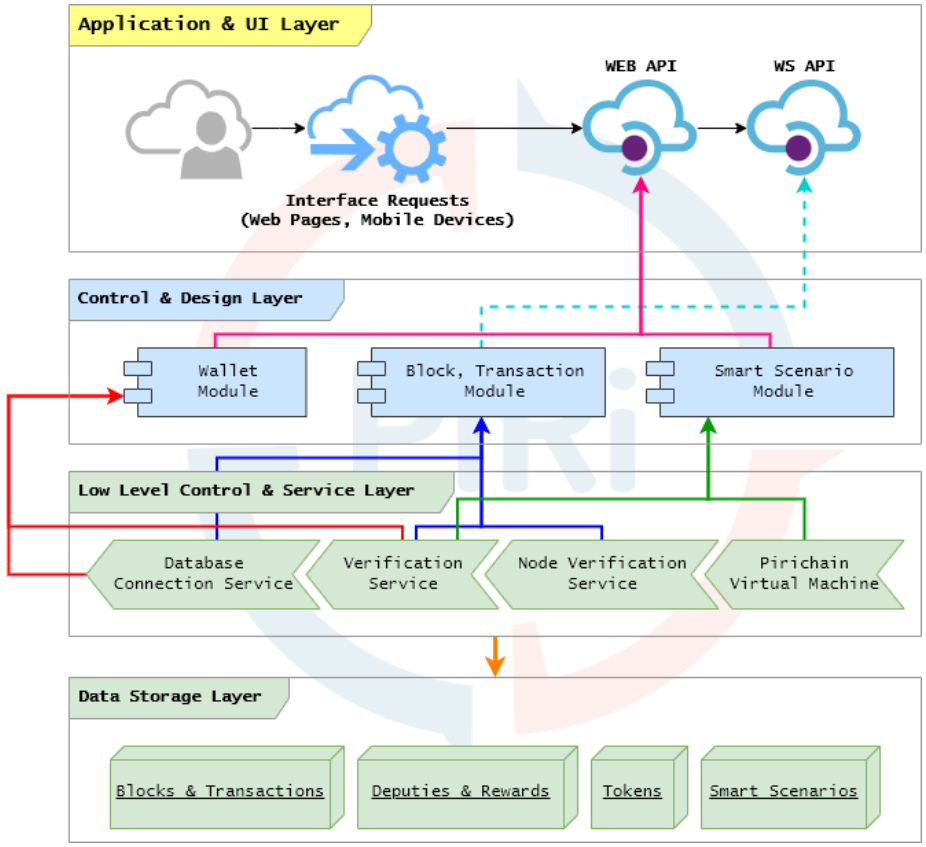


Figure 1.9: Piri Blockchain database and service structures

1.7. Consensus at Pirichain

In Pirichain, at least 80% of the validators and at least 50% of the core nodes are required to be approved. Apart from this situation, every action that will destabilize the system is reported to the servers, and the protocol to investigate the incompatible nodes is started.

Opportunities for companies to set up their own nodes in their locations are possible under certain conditions/contracts. 500.000 PIRI Coins are taken from companies as collateral. The contract is terminated if it is determined that the Byzantine fault tolerance is not complied with. Even if the contract is terminated, the guarantee is not paid back in the first year.

Performance Measurements: Since the queuing module will be activated in case of exceeding a certain traffic in the system, the load on the nodes remains constant after a certain value. This prevents the system from behaving inconsistently. The processor (CPU) undertakes the greatest load on the entire system. The reason is that there are many cryptographic operations. Since there are Process Queuing, Garbage Collector and Single Thread - Context Switch features on the ram, no bottleneck has been observed in 4 and a half million transaction records.

In tests on the system, a maximum of 190 thousand transactions were provided in one day. And 77% of them were retrieved and processed via queuing. During the recording of these transactions, it was observed that a maximum of 184 transactions joined a block period (10 seconds), and no inconsistency was observed in the number of transactions of the nodes.

Another situation expected from the system is the need to calculate the balances very quickly (maximum 150 ms). However, as the number of transactions in the system increases, the calculation time is expected to be delayed. As a result of the indexes added to the database, there is a slowdown of 400 ms after 600 thousand transactions. This delays the processes in very heavy traffic on the system, especially in data addition. In order to avoid this undesirable situation, there is a table on the server and nodes where only the balances are kept on the database side. Via this table, very fast transactions can be made. The flow chart showing the update process of this table is given in Figure 1.10.

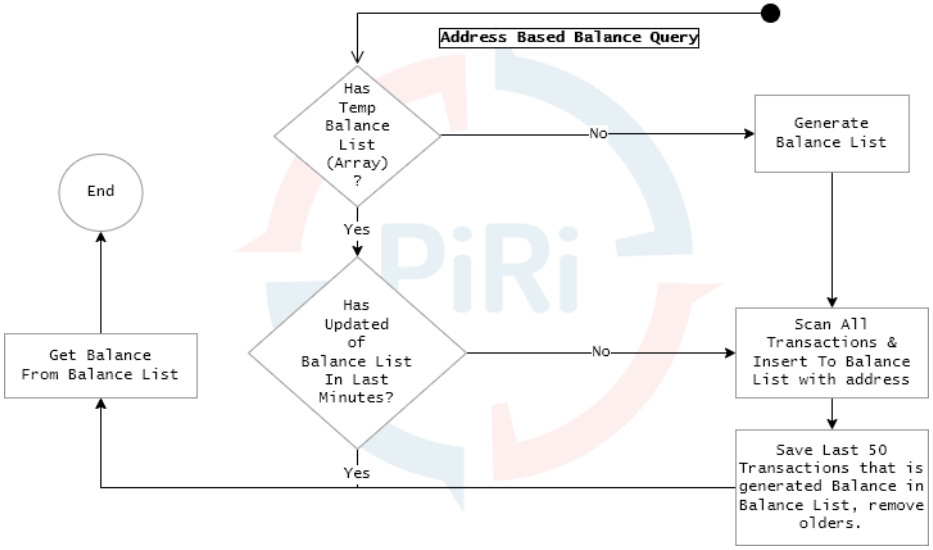


Figure 1.10: Piri Blockchain balance control flow diagram

2. PIRICHAIN SMART SCENARIO

Pirichain smart scenario system has capacity of analyzing and processing data on the basis of typescript and javascript. The information has been added by the companies to allow the queries that the companies want with the smart scenarios written by the software experts. Besides query, it is possible to run different scenarios by creating certain conditions. The diagram in Figure 2.1 shows the relationship of smart scenarios with the whole system. In addition, the actions that smart scenarios can do on the system are also explained in the boxes in the diagram.

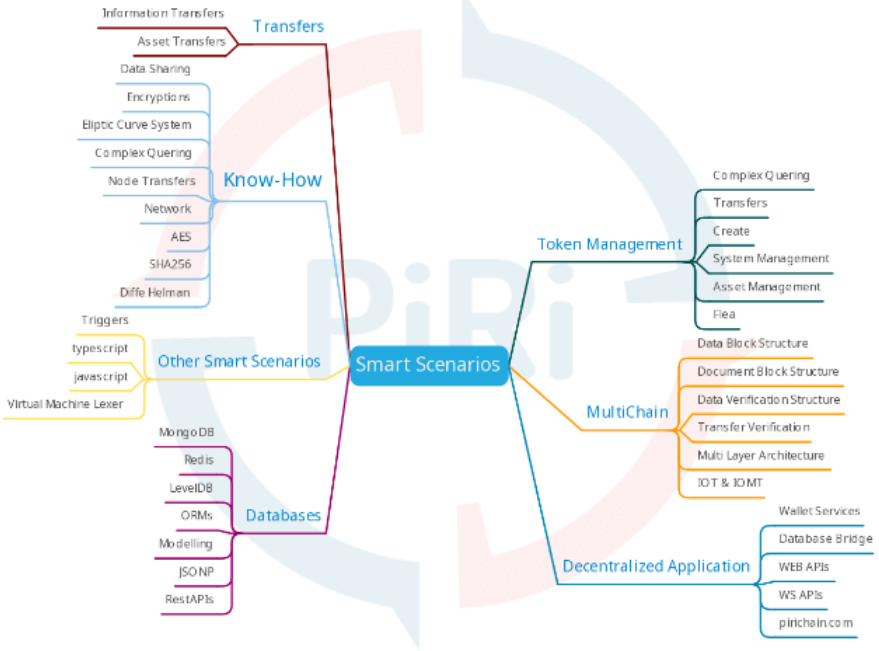


Figure 2.1: Pirichain Smart scenario relationship with modules

Pirichain smart scenarios undertake tasks that cover the entire system. According to the scenario structure to be written on the system, whether information transfers are made or the assets are sent to the desired addresses according to a certain condition, this completely changes according to the modeling to be determined by the users.

As the simplest form of expression; information added to the block network, flour, water, sugar, oil etc. Considering that they are products, either pies or breads can be made with smart scenarios. This is entirely up to the developer's own needs and abilities. Whatever the software requirement analysis requires, the desired data modeling can be done with Pirichain's ready-made functions, and the needs can be shaped with complex queries. Pirichain scenario development interface is shown in Figure 2.2.

```
async function init(param1,param2,param3)
{
// Your code goes here...
// You can execute only you

if (EXECUTER_ADDRESS!==OWNER_ADDRESS)
return "This scenario  executes only owner";


var filterData=Transaction.findDataWithValue(EXECUTER_ADDRESS,{'name':param1},
                                             {'surname':param2},0,10);
if (filterData)
{
    return {message:"Data has been found"};
}
else
return {message:"Data has not been found!",data:null};

}
```

Figure 2.2: Pirichain interface scenario development area

2.1. Pirichain Smart Scenario Virtual Machine

Commands to be included in the system are made ready to be run in the system after lexer design, syntax and semantic controls by Piricihain Virtual Machine. In addition, malicious (devil codes) codes for locking the system from the logical side are detected (if found, they are reported to the Pirichain system) and bad codes are extracted.

Each scenario code written on the system is given an execution time of maximum 50 seconds. Every process that has not finished running (throwing runtime timeout error) within this time scale is canceled. Each canceled scenario is administratively reported by the server. A certain number of scenarios that tire the system (receiving a timeout error) are removed without notice. Addresses that frequently repeat the same situation in the system are blocked regardless of the balances of the assets in them. These addresses cannot operate in the system and cannot access the system. An example of cross-scenario work is briefly shown in Figure 2.3. The data sent by the user with a certain balance in the scenario is sent to Scenario B. Before Scenario B is run, "Scenario Execution Authorization" is checked. Otherwise, the Program is terminated. If available, it is sent to Scenario C and Scenario C is run. The program is terminated without running any scenario for the user with no balance.

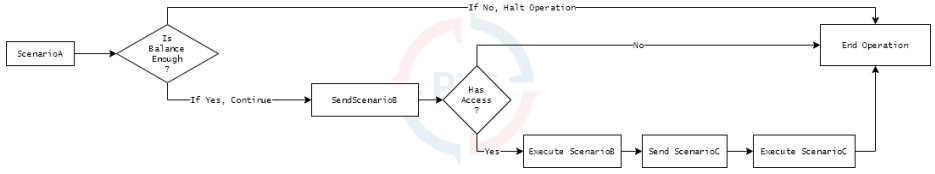


Figure 2.3: Working example between scenarios

In Figure 2.4, a structure constructed between scenarios in detail has been created. As seen in the structure, it shows that the data requested from the school and the Ministry of Education of a student applying to X university is run on the scenario of X university.

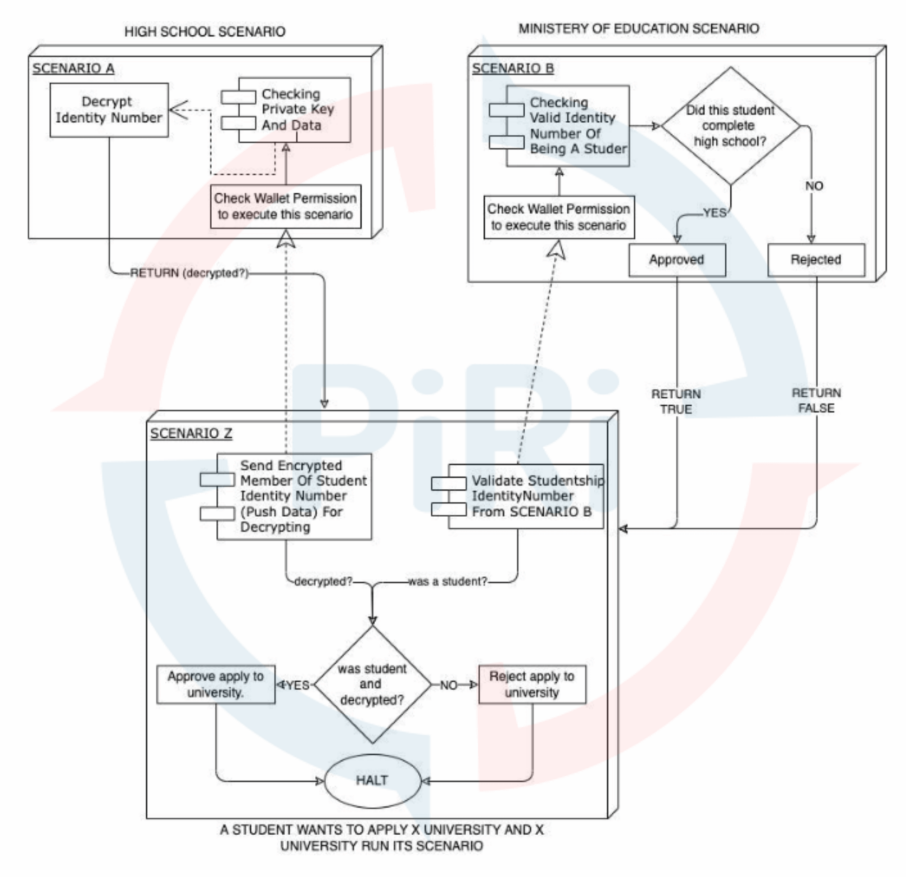


Figure 2.4: Detailed operational view of scenarios

2.1.1. Pirichain Example Smart Scenarios

2.1.1.1. A Scenario on Health

The relationship diagram established between the Patient-Doctor-Hospital-Pharmacy-Health Insurance Company and the Ministry of Health is shown in Figure 2.5.

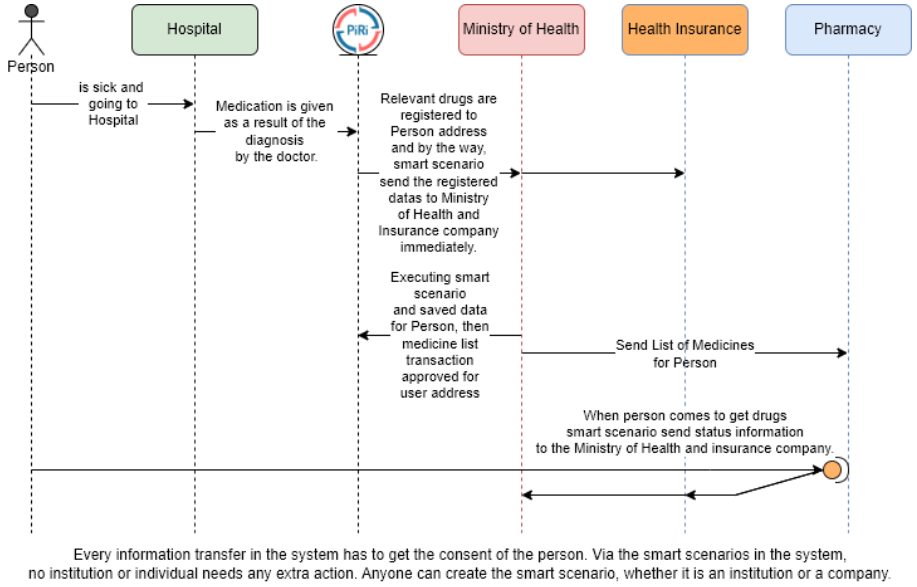


Figure 2.5: Patient-Hospital-Ministry of Health Pirichain Smart Scenario Diagram

As seen in Figure 1.13, each unit is directly or indirectly interconnected with the other unit. Every connection is made with addresses. Data is transmitted to each unit in encrypted form. Every data transfer in the system is stored by the nodes. If desired, nodes can be established both on the ministry side and hospitals.

After each data and transaction sent in the scenarios, it may be sent to the 2nd or more scenarios. This allows a chained group of transactions to run with a single transaction. From another point of view, every smart scenario written in the system; In fact, it has a structure that can act as a trigger and provide connections like graph structures, and can change state according to the condition, similar to a finite state machine.

2.1.1.2. A Scenario on Inventory

Example of Stock-Inventory-Branches scenario is given in Figure 2.6. According to this scenario, data transfers between addresses within the company and transfer to smart scenarios are displayed after the product is entered into the company.

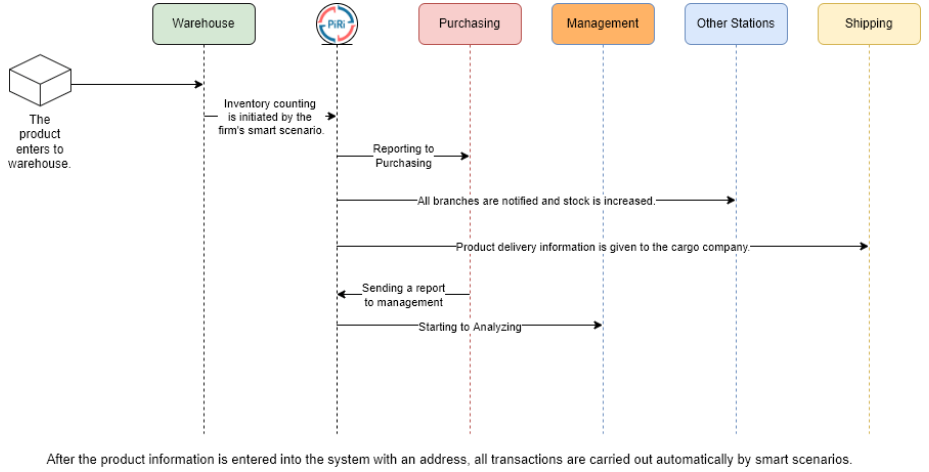


Figure 2.6: Product Entry and Transactions within the Company

2.1.2. An example setup in Pirichain within the Company: Scenario of calculating the semester average with course grades and coding example:

As seen in Figure 2.7, the course name and course grades of the student were sent to the block via different transactions.

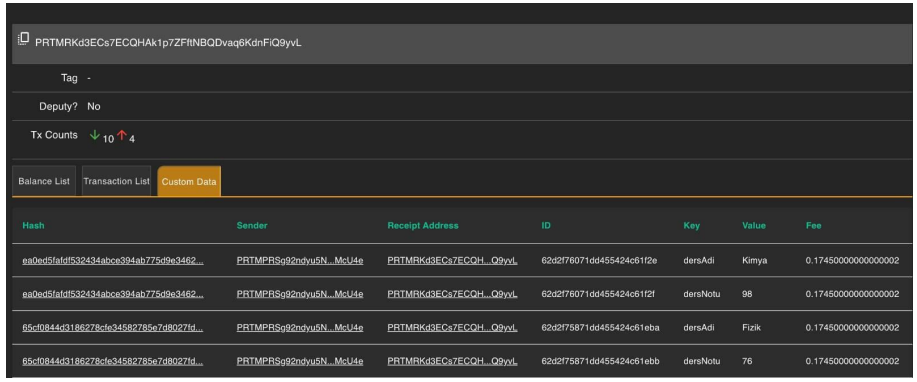


Figure 2.7: The course information of the student has been sent to his/her own address.

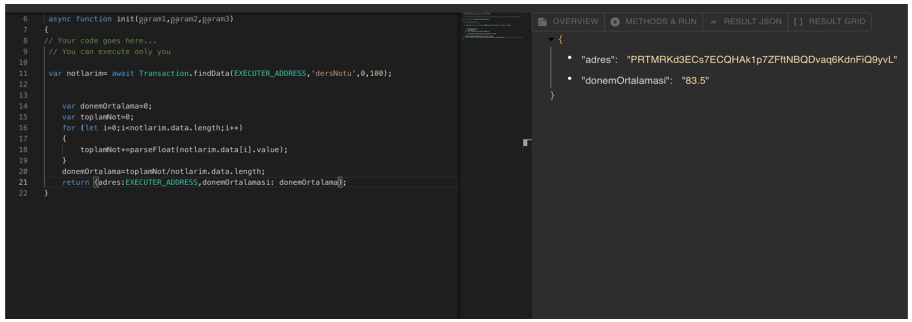


Figure 2.8: Smart scenario coding that finds the semester average

As seen in Figure 2.8, the smart scenario was coded upon calculating the student's semester average. All lecture notes of the student sent to the block network beforehand are shown in Figure 2.9.

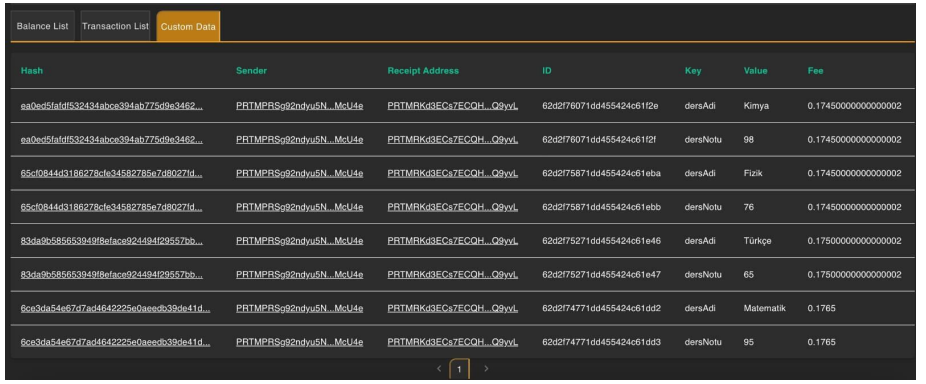


Figure 2.9: Entire list of grades

These grades are intended to be averaged with a small scenario as in Figure 2.8. Coding was done in javascript format on the left side of Figure 2.8. As can be seen on the right, the period average (period average: 83.5) is calculated by the system

3. Pirichain Platforms

3.1. Pirichain Desktop Wallet & Database Bridging Application (Pirichain Wallet & DataBridge Application)

Pirichain desktop application is designed for purely commercial use. In practice; In order to send bulk data, it is ensured that the data is sent to the Pirichain block network in bulk by connecting to the company's database through the application.

6 different database types (MSSQL, MySQL, Oracle, PostgreSQL, MongoDB, Sqlite) can be connected via DataBridge. The records to be sent after the connection can be selected by querying with SQL language or the records in the whole table can be selected and sent to the Piri Blockchain network.

4. Pirichain Transaction Types:

Asset transfer transactions: As the name suggests, it is sending coins or tokens between addresses in 2 base58 formats.

Pushing data to the block network: It is the sending of companies or individuals' own data to the block network, either encrypted or unencrypted.

Data sending to smart scenarios: Used for processing data of end users. Data or assets sent to smart scenarios can interact with other scenarios. Entity or data can be sent from one scenario to another scenario. Thus, it is being developed as a system with Turing completeness (Turing Integrity, Wikipedia). Figure 4.1 describes the relationship between them.

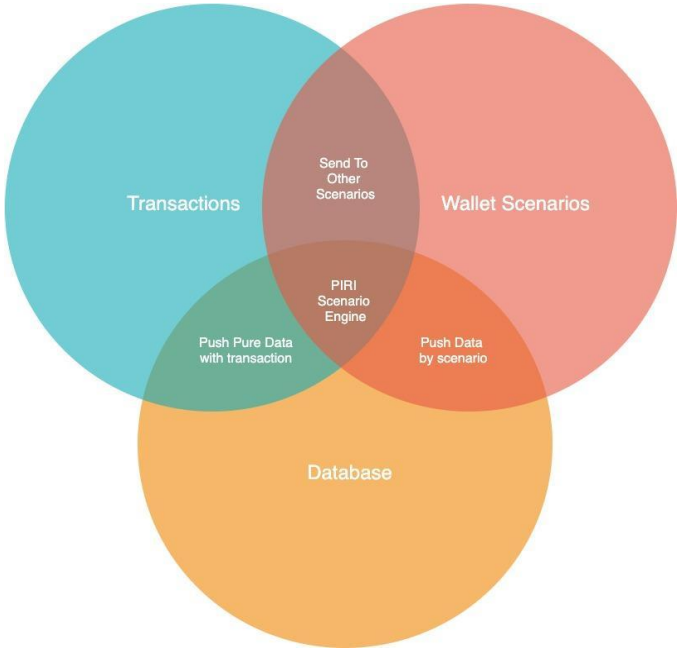


Figure 4.1: Operational relationship between Transactions and Smart Scenario

5. Pirichain Commission

Pirichain applies a PIRI deduction of 0.1 between asset transfers (coin or token). For data upload to the block network; 0.0005 PIRI commission is deducted from each added character (8 bits).

6. Pirichain Reward Distribution

Working according to the dPoS reward distribution center, Pirichain is eligible to receive rewards when representatives freeze at least 1 million PIRI coins from delegates. The reward per block is 10 PIRI. The first 7 representatives with the most coins frozen will receive a prize. Delegates are given daily prizes.

Block Opening Reward: 20% of the daily total block gain is burned. 20% of the remaining prize is given to the representatives. The remainder is distributed to the delegates, taking into account the following formula.

Deputy (Representer) Reward:

$$Wc \Rightarrow Number\ of\ Produced\ Blocks$$

$$Wc = 6 \times 60 \times 24 \Rightarrow 8640$$

$$K_i \Rightarrow Number\ of\ Blocks\ Caught\ by\ Deputy$$

$$Q \Rightarrow Reward\ on\ each\ block\ (10\ PIRI)$$

$$Daily\ Reward = \sum_{n=1}^{Wc} \frac{K_n \times Q \times 16}{100}$$

Delegation Reward:

$$Delegation\ Max\ (Daily) = \frac{1}{365} \times \frac{1}{1000} \times Frozen\ Amount$$

$$Daily\ Total\ Max\ Reward = Wc \times 10 \Rightarrow 86.400\ PIRI$$

$$Delegation\ Daily\ Reward = \frac{K_i \times Q \times 0.64}{7}$$

$$f(x) = \begin{cases} \text{DelegationMaxDaily}, & \text{DelegationMaxDaily} < \text{DelegationDailyReward} \\ \text{DelegationDailyReward}, & \text{DelegationMaxDaily} \geq \text{DelegationDailyReward} \end{cases}$$

As seen in the f(x) function above, the highest number of awards the delegation can receive has been calculated.
WEB-API Detailed Documentation: http://tiny.cc/pirichaindocs

7. PIRI Coin Holders

Total PIRI Supply	14,571,923,386
Firms Reserved (For Commercial Use Only)	4,225,857,781.94 (29%)
Individual Use PIRI Reserved (The maximum supply of cryptocurrency exchanges)	10.346.065.604.06

Chart 7.1: Piri Coin Distribution

PIRI COIN Commissions	
On Each Transfer	0.1
Added to the PIRI Block network on each character	0.0005 PIRI

Chart 7.2: Piri Coin Commissions

It aims to provide an indispensable Blockchain-based service (Blockchain as a Service) in the market.

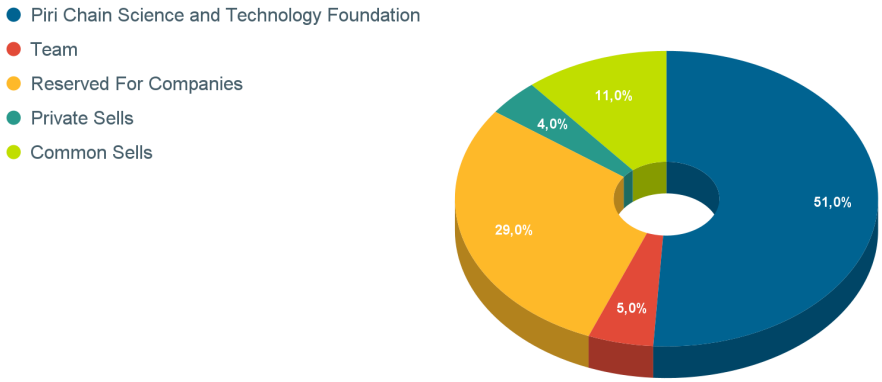


Figure 7.1: Piri Coin Distributions

Pirichain Science-Technology and Humanitarian Aid Foundation will be established in 2023. And its wallet will be active in the 3rd Quarter of 2023. A 10% PIRI Coin Sale will be allowed to the foundation within a maximum of one year from 2023 to 2025. It will be able to use PIRI coins for humanitarian aid and projects developed under science-technology. The revision given to the companies will not be in the market. It will only be used for the service that companies receive through Pirichain.

Private sales will start in August 2022 and sales will generally be made to companies. PiriEx Cryptocurrency exchange (https://www.piri.exchange will start in August-September

8. Pirichain Projected Roadmap (Pirichain Roadmap)

August 2022	**Pirichain Beta Release** System Testing ends and beta launches.
2022 September - October	**Private & Public Sales Special sales** Piri will sold for commercial wallets in pirichain.com "BUY PIRI" area and personal wallets can buy https://piri.exchange
2022 November - December	**Service to Commercial, Private Institutions Introducing** The Pirichain "Database Bridge" application and WEB-API for uploading pirichain data to the international market
2023 January - March	**PIRI Listing Application to Global Exchanges For listing PIRI** Coins on crypto exchanges with high volume ratios around the world start of applications
June 2023	**Stable Coins to PIRI Network** (USDT, USDC, etc.) Applications of stablecoins integrated into Pirichain block network and infrastructure work.
2023 September	**IoT and IomT Integrations** Establishing the necessary infrastructure for devices working in the internet of things to use the PIRI block network
2024 March	**Information Ecosystem in the Global Market in All Languages** To transform the data ecosystem formed by the data records of companies into an information ecosystem for Pirichain smart scenarios. To serve all companies globally in this infrastructure.
August 2024,	**Firm-Specific Data Ecosystem** Creation of firm-specific blockchain networks that will be integrated and synchronized with the Piri blockchain, whether public or private sector companies, and the introduction of multichain..
January 2025	**Encouraging of Pirichain Integration with Artificial Intelligence Fields** Companies to use Pirichain infrastructure as the data warehouse of the system in order to support and serve artificial intelligence studies.
2026	**Being in the Top 3 Global Brands in the Information Ecosystem and Baas (Blockchain as a Service) Technology.**

REFERENCES

1. Walker, G., 2020, BIP39, https://learnmeabitcoin.com/technical/mnemonic (Access: 01.07.2022). (Walker)
2. Turing Integrity , https://en2en.wiki/wiki/Turing_completeness (Accessed July 21, 2022)
3. https://www.reddit.com/r/Bitcoin/comments/eelqdo/number_of_bip39_seed_word_combinations_vs_atoms/
4. https://learnmeabitcoin.com /technical/mnemonic