WHITEPAPER

PZM CASH

Cryptocurrency with algorithm of consensus Proof - of - Stake

Version March 2020

Table of Contents

1. Introduction

PZM Cash is a cryptocurrency created as a means of payment for a fast-growing digital ecosystem in which the economic motives of each individual participant provide an increase in the overall wealth and wellbeing of the entire community. The main strategic success factor for PZM Cash is the fact that it will be relying on the growth of scaling and balancing of supply and demand for funds.

Advantages of the PZM Cash architecture:

- Sidechains providing security for the main ledger;
- Proof-of-Stake consensus algorithm;
- A large number of functions and development opportunities for developers of decentralized applications (dApps).

The PZM Cash team has significantly upgraded the PoS consensus algorithm that had been used earlier. The commission for transactions in the PZM Cash network is fixed, which guarantees the fair distribution of remuneration among the forgers.

The key difference between PZM Cash and the “classic” PoS concept lies in the mechanism of ensuring the network with monetary supply. The PZM Cash team refrained from a full emission approach when generating the first block. Only 1% of the total number of coins will be distributed when the network is launched using pre-mining. The remaining coins will be issued during PoS mining as incentive payments to loyal PZM Cash holders for supporting the network.

The forgers will receive transaction fees for adding blocks to the main network chain. At the same time, the chance of adding a block linearly depends on the size of the assets located on the wallet – the current stake of PZM Cash. No additional payments for forging, other than the commissions, are provided for, as all emissions after the launch of the network will be made through PoS mining.

The PoS mining mechanism has two main components:

- The leading activated wallet;
- The supporting wallets – wallets activated by a transaction from a leading wallet.

Remuneration payments are made to the leading wallet. However, their size is determined by the balance of the leading wallet and the balances of all supporting wallets. Moreover, the number of coins on the balances is the only factor affecting payments. There will be no changes in the size of payments over time.

If the size of the stake on the wallet reaches 0.011% of the total amount of coins issued (1,000,000 PZM Cash), the PoS mining process is halted. The network is thus protected against the risk of over-centralization of assets.

The remuneration of users for loyalty through PoS mining provides the network with a solvent user base and generates demand for services in the PZM Cash ecosystem. In addition, the orientation of the architecture on the convenience of dApps development with a broad spectrum of functionality will ensure the emergence of a wide range of services and use cases through the creation of a large number of independent applications.

The implementation of PZM Cash in JavaScript expands the possible range of third-party applications even further, since the relative simplicity of the language allows multiple developers to join and expand the functionality of the PZM Cash ecosystem. It also allows for a significant expansion the functionality of browser solutions related to PZM Cash.

The final advantage of PZM Cash, which is provided through the use of JavaScript, is the ability to use the Web3 js wallet solution. Thus, a wide range of partners will have access to their balance sheets and unify PZM Cash as a payment instrument.

2. Product and Use Cases

PZM Cash is, above all else, an international, independent and transparent means of payment.

Each user, regardless of their location, can carry out transactions, and, if desired, participate in network administration by deploying a node and installing the necessary software.

Any PZM Cash user can use two cryptocurrency usage scenarios: passive and active. The two cases differ in the degree of participation in the development of the network.

- Under the passive participation scenario, the network participant is a simple user.
- Under the active participation scenario, the user is also a network administrator (forger) and takes an active part in its development and expansion.

As such, there are two types of participants in the network.

- Ordinary users who use hot wallets (in a web environment). They do not allocate space for the needs of the network on their computers, do not deploy nodes and receive income solely for holding PZM Cash on their wallets.
- Forgers, who receive income from forging – by adding new blocks to the network chain.

Use Cases

Passive Use Case Scenario

The given scenario assumes that the client uses a browser (web) version of the wallet (hot wallet), which allows for the implementation of some main functions in the form of transactions on the network, including the execution of smart contracts.

A registered and activated wallet allows the client to receive income in the form of additional coins accrued in accordance with the two-factor PoS mining algorithm. The more coins there are on the user's wallet, the higher their reward. More information on the accrual factors can be found in the corresponding section.

The browser solution allows users not to allocate space on their hard disks for the needs of the blockchain and not to deploy a full node.

For the passive use case scenario, the participant needs to:

1. Create and activate a hot wallet on the PZM Cash website. The wallet is activated through an incoming transaction.
2. The PoS mining process will be launched the moment the minimum value of 1 PZM Cash is transferred to the wallet’s balance.
3. The amount of additionally transferred PZM Cash depends on the PoS mining factors (the balance of the leading wallet and the total balance of the supporting wallets).
4. The user can exchange the surplus coins (excess liquidity) for any other currency they desire on cryptocurrency exchanges and diversify their digital assets portfolio, or use it to pay for dApps and transactions.

Active Use Case Scenario

The passive use case scenario assumes that the user takes an active part in building the network by adding new blocks and records to the ledger and confirming them, thus synchronizing and administering the blockchain.

The participant receives income in the form of a forger commission for confirming the transactions of other users and adding new blocks. The income consists of a percentage of the amount of transactions in the block.

In order to implement an active use case scenario, the participant needs to:

1. Deploy a full node and allocate space on their HDD and install the specialized PZM Cash software for computing the blocks.
2. Keep as many PZM Cash coins as possible on their balance. An increase in the number of coins on the balance increases the chances of adding a block.
3. Maintain the node in online mode, create new blocks and build blockchain branches containing hashed transaction records.
4. Receive remuneration for confirmed transactions in the form of a commission fee, which is a percentage of the transaction amounts (forging).

When a node is deployed, the administering account obtains the right to add new blocks to the PZM Cash blockchain (forging). If a transaction is made at any point in the world during the formation of a block and enters the given block from the pool of unallocated transactions, then the administering account that generated the block receives a fixed commission for the transaction. The amount of commissions for all transactions in the block is the forger's remuneration accrued to the account that formed the block.

The greater the balance of static PZM Cash coins on the wallet and the longer the new block is not added to the blockchain, the higher the chances of the addition of a new block to the blockchain by any specific account.

The PZM Cash Wallet

PZM Cash wallet is a universal tool for managing coins on the balance of each unique user account. The wallet allows users to conduct outgoing transactions using the user's private key and generate details (public keys) for receiving transactions from other users.

Wallet Functionality:

- Carrying out p2p transactions;

- Conducting transactions during the execution of smart contracts;
- Creating smart contracts using templates;
- Providing access to decentralized applications of the PZM Cash ecosystem;
- Displaying the balance of the wallet and the dynamics of its transactions.

The blockchain's cryptography is based on asymmetric encryption. This means that each wallet has public and private keys. The digital keys are records in the form of a set of characters that control access to the assets and coins stored on the wallet.

The digital keys are always paired. Each wallet has a private and a public key. The public key is required to identify the wallet on the network and is used as a requisite for receiving incoming transactions.

The private key is used for signing outgoing transactions and transferring coins to other wallets on the blockchain.

The private key is responsible for controlling the coins on the wallet and therefore should always be under the control of the account holder.

In addition, the digital keys are created and stored by the users, or can be generated and managed by the user's wallet software. They are therefore completely independent of the blockchain protocol.

When first accessing to PZM Cash, each participant must use a web client (browser access) and create an account by simply generating a private key.

The private key is generated on the basis of the data entered by the user the first time they access their personal account on the website. Users must either confirm the displayed field in which the private key is indicated as a symbolic record, or enter the character set by themselves. A private key will be generated upon confirmation of the entered data.

The private key must be written down, because it is unique and cannot be regenerated. If the private key is lost, it will be impossible to enter the account and the wallet will become inaccessible. It is the private key that gives users access to the wallet. The private key is similar to a digital signature, and it is thus recommended users store it on portable storage drives or on a local disk.

Users then need to activate the wallet on the PZM Cash website. This will allow users to make full use of the functionality of the wallet, carry out transactions and participate in PoS mining.

To do this, users need to generate a public key. The public key represents the transaction details that other users will need indicate to transfer coins to another user's wallet. After the first transaction to the wallet is confirmed (the transaction information will be recorded on the blockchain), the user's wallet will become fully operational. The public key is stored in the verification data branch along with the data eligible for verification.

To receive and send PZM Cash, users need to use two more elements that are generated from the two aforementioned keys. One of them is the address. An address is a string of numbers and letters created from the public and private keys and represents a "fingerprint" of the given keys. Since private and public keys have a complex format, they are converted to a more simplified format using a mathematical algorithm for the convenience of the users. The public and private key versions are called the public and private addresses, respectively.

The private address provides access to the account and, accordingly, access to the coins, while the public address is the wallet number, using which other users can transfer coins to other users.

To create an outgoing transaction, users must first verify the ownership of the coins in the transaction. To do this, it is necessary to prove that the user knows the secret key. A digital signature is used for these purposes. Signatures are cryptographic elements that are calculated from the private key and a set of other information included in the transaction, which is entered by the user creating the transaction. Therefore, the signature is a confirmation of the desire to carry out an outgoing transaction and is thus unique. Since signatures are calculated using the private key and a set of other transaction information, they also prove the knowledge of the secret key and the right to confirm the data in the transaction. Therefore, each signature is valid for only one specific transaction.

Web 3 js

The implementation of PZM Cash in JavaScript enabled the use of Web3js technologies, which significantly expanded the capabilities of the PZM Cash Wallet thanks to unification. The wallet can be used on the platforms of our partners, for example, on exchanges and in casinos, without creating a separate wallet for each project. Moreover, the browser implementation eliminates the need for a blockchain core for integrating new channels.

Web3js is a collection of JavaScript libraries that allows remote interaction with a node via HTTP or IPC connection, which simplifies the integration of the PZM Cash Wallet through a dedicated API. As a result, partner platforms do not need to deploy a full node to ensure integration.

Smart Contracts

Our wallet allows users to send transactions not only to the addresses of other network participants, but also to the addresses of smart contracts by initiating various transactions based on a digital algorithm.

Smart contracts are digital protocols that use mathematical algorithms to automatically complete a transaction after some established conditions are met. The process is completely controlled by the logic of the algorithm, and therefore, the participation of a third party is not required for the execution of the smart contract, which acts as the guarantor of the invariability of the code. The invariability of the code itself is guaranteed by the writing of the code of the smart contract on the blockchain the moment the code is created. A smart contract is activated by an incoming transaction, which extracts it from the blockchain and receives the necessary data.

In order to access a smart contract, the user needs to create an outgoing transaction to the address of a specific contract. The transaction will be executed the moment it is confirmed.

The obligations of the participants are stipulated in the form of a “if – then” scenario – a transaction. For example: “if A transfers digital funds, then B transfers the rights (in digital form) to any asset.” A corresponding entry is made in the blockchain, which becomes immutable. By resorting to the given data entry, users can always confirm any user’s right to any asset and the fact of the transaction’s occurrence.

A smart contract receives information regarding digitized rights to an asset from an external source, and each blockchain node executes smart contracts independently. This means that each node receives data from an external source on its own. However, in order to avoid any conflict in the blockchain and achieve consensus, each node must receive the same and immutable response from an external source. The facts are confirmed by the “oracles”, which are a software layer between an external source and a smart contract located directly on the blockchain.

The smart contract does not directly contact the external source, but the corresponding oracle, which creates an incoming transaction that writes the necessary data to the ledger. Thus, each node receives an identical copy of the data, and the execution of the smart contract becomes possible.

3. Technical Implementation – The Core

When referring to the “Core” of the cryptocurrency, or the kernel, users need to keep in mind the specifics of the consensus algorithm and the blockchain protocol, and understand that the two are completely different things. The protocol is the architecture and the primary rules governing the blockchain, while the algorithm is the mechanism through which the rules will be implemented. While the protocol defines the rules, the algorithm tells the system what measures should be taken to comply with all the conditions of these rules and obtain the desired results. In other words, the protocol is a “static” network, and the consensus algorithm is responsible for its dynamics, which include the introduction of changes to it and the acquisition of new states by the network according to the protocol.

The Protocol: The Distributed Ledger and The Nodes

The blockchain is a database (ledger) implemented through the concept of an interconnected list, in which each new record contains information about the previous one in encrypted (hashed) form. The ledger provides a permanent record of transactions that have taken place, and also establishes the order in which the transactions were made. The main advantage of the blockchain is its resilience to any changes. If any block is changed (for example, as a result of an attack), then all subsequent blocks will automatically be changed, which leads to the instant detection of any attempts at forgery.

The PZM Cash cryptocurrency is implemented on the blockchain and is focused on the development, improvement and expansion of the functionality of decentralized applications. Unlike Ethereum and other blockchains that use specialized programming languages for creating decentralized applications and launching smart contracts (for example Solidity), PZM Cash uses the much more common and simpler JavaScript. This feature makes the platform accessible to a large number of developers and provides the scaling and development of use cases. In other words, users do not need to learn any special languages in order to develop their own decentralized applications (dApps) for PZM Cash.

The use of JavaScript allows to provide developers with a large number of special libraries that facilitate development in the fields of cryptography, transactions, P2P, etc. Each library complies with the ZPM Cash protocol. Thus, PZM Cash is conceptually designed for a broad audience of users.

The main distinguishing feature of the blockchain is the use of sidechain technology for running fully debugged applications and independent blockchains within the same platform. Sidechains are standalone ledgers implemented on top of the main ledger. The sidechains do not affect the size of the main network.

The application of such an approach allows for achieving:

1. Unlimited scalability – the use of sidechain technology allows users to scale the network infinitely.
2. Increased network security – given the fact that sidechains are located on top of the main network, it is therefore impossible to disrupt the latter by creating bugs in "subsidiary" networks or violating the stability of their operation. For example, if an error occurs in the Ethereum network, a hard fork is required to fix it.
3. Expansion of development capabilities – developers can experiment with their applications on sidechains without fear that any errors will disrupt the operation of the main network. Each project (dApp) is created in a separate sidechain, so developers have ample opportunities to customize their applications as they see fit.
4. The implementation of sidechains allows users not to deploy a virtual machine for eliminating bugs. For example, the deployment of a VM is required for eliminating bugs in the EVM (Ethereum Virtual Machine).

The platform also provides decentralized file storage and escrow services for smart contracts. The oracle service confirms information about events that have occurred or are ongoing.

Users are provided with a catalog of decentralized applications, including for portable devices: smartphones, tablets, etc. Each utility is registered on the main chain, and clients can see all the applications and services available on each sidechain. Users receive access to all decentralized applications in one place, much like GooglePlay or the Apple Store.

An important distinguishing feature of PZM Cash is PoS mining – an algorithm for ensuring the network with additional liquidity in addition to the initial coin genesis.

The developers of PXM Cash fully understand that this is a fairly aggressive model for increasing the money supply, and have thus chosen a kernel that was originally designed for creating additional use case scenarios. The balance of the supply and demand for PZM Cash coins is thus achieved in order to avoid the development of inflationary mechanisms in the ecosystem and the depreciation of the exchange rate.

The main blockchain contains the hashes of the sidechains. The hashes are records encrypted in a special way that allow users to check the integrity and authenticity of the original record, but do not make it possible to decrypt it. This is done in order to increase the required speed of the network.

Each PZM Cash block contains the following information:

1. Information about the block

- Block version and unique block identifier;
- Block timestamp expressed in seconds;
- Identifier and cryptographic hash of the previous block;
- Information received from sidechains;
- Network Status Metric (Nugget);
- ID of the account that created the block, as well as the public key of the given account needed to identify it.

2. Transaction Information

- The number of transactions stored in the block;
- Transaction data. Data of all transactions included in the block, including their identifiers;
- The total amount of PZM Cash on transactions included in the block, including the amount of commissions;

- Data on smart contracts. Information on the status of the smart contracts;
- Block payload length and hash value of the block payload;
- The value of the forging bar and the cumulative complexity for the block.

The PZM Cash Node

A blockchain node is another architectural element without which it is impossible to imagine a blockchain. The presence of many independent nodes allows users to create a network with a distributed (decentralized) structure. The idea is that each independent device stores the current version of the ledger on a dedicated HDD. As such, any device with PZM Cash software installed on it is considered to be a separate node.

In this case, the nodes are synchronized. If there is a malfunction in even an insignificant number of nodes, the remaining nodes will indicate an error. Thus, in order to carry out an attack on the blockchain, an attacker needs to synchronously change the necessary data in a huge number of nodes, which becomes increasingly difficult as the network grows.

Each node in the PZM Cash network has the ability to process and transfer transactions and information in blocks. Moreover, the nodes are synchronized with each other, as they contain identical records of the current state of the blockchain. This leads to the exclusion of the possibility of a double spending error, which means that the same coin can participate simultaneously in different transactions.

PZM Cash uses a two-level node structure:

1. The Full Node

A full node is a device with the PZM Cash software installed on it, which stores the full and current version of the blockchain. A full node can act as a consensus node for participating in the creation of new blocks and forging. The administrator of a full node can take an active part in the formation of the blockchain, constantly grouping incoming transactions into blocks and distributing them over the network.

A full node also acts as an audit node. In this context, a node regularly checks and confirms the forging results of other nodes and distributes the load across the network, thus acting as a kind of content delivery network (CDN) for blockchain data.

2. Light Clients

The second type of nodes are light clients. They are called light clients, because they do not have a full version of the blockchain and contain only the data that is important for the node, which allows users to limit the required amount of memory allocated on their HDD and the necessary processing power. For this reason, they are a good option for setting up a dedicated cryptocurrency wallet.

The light client stores only the data that is required for implementing custom use cases. For example, such a light client allows users to generate transactions and track the balance of the wallet. If the user does not need anything else, their device will not be loaded with any excess or unnecessary data.

A light client can work on mobile devices or via a user’s account on the PZM Cash Wallet website. At the same time, users do not store a local copy of the blockchain, since to send transactions. It is sufficient to store the private keys with which these transactions are signed.

However, unlike with other cryptocurrencies, users of the PZM Cash light client can receive rewards for supporting the ecosystem. A light client cannot participate in forging and adding new blocks, but the PoS mining algorithm ensures a steady flow of new coins to the balance of light wallets.

The Consensus Algorithm

The main process for the network is the transaction process, which is technically related to the addition of new blocks to the ledger. The addition of a new block is carried out according to a certain consistent algorithm, which is the consensus algorithm.

The consensus algorithm allows users to establish and confirm the validity of each operation, as well as synchronize the blockchain version on all nodes. Moreover, it should provide the same "point of view" on the blockchain by each node, considering that some nodes can hang up, lag or fail altogether. The algorithm is also designed to protect the system from unauthorized access, the altering of the list of past transactions and hacker attacks. The algorithm is guided only by the general rules for processing messages on the network when performing its duties.

The consensus algorithm ensures the dynamics of the system, its development and growth, while preserving the unique properties of the blockchain, such as the equality of nodes, as anyone can participate in by adding blocks. Objectivity is also ensured and users do not need to trust certain third-party sources, since the blockchain itself provides for confirmation of validity in algorithmic form.

At the same time, consensus is constantly ensured, as each node in the network reaches the same state after processing each transaction and each block. The consensus algorithm ensures that all the nodes of the network always have the same version of the blockchain and this eliminates the possibility of any conflicts between the nodes.

The consensus algorithm determines the conditions that need to be fulfilled by a network member having the right to add a block to the network to be able to place the block they formed in the ledger in primary order. Thus, the given block will be recognized by the network, a consensus will have been reached on the network about its new state, and the "author" of the block will receive a reward.

There are many different consensus algorithms that differ from each other by the necessary condition and what is considered to be the fulfillment of the condition. The most popular of these are the Proof-of-Work and Proof-of-Stake.

The Proof-of-Work algorithm requires the author of a new block to solve a mathematical problem, and this problem can only be solved by direct enumeration of the possible values. The classic option is to find a special value for the hash of the block header containing a link to the previous block. This approach is implemented in the Bitcoin blockchain.

The mathematical problem is solved by all those seeking to add a block. The chance of solving the problem faster than others and, accordingly, receiving a reward, depends on the amount of available processing power. The greater the processing power of the node – the higher the chance of getting the reward. At the same time, the necessary processing speed is ensured by the selection of the complexity of the problem to be solved, depending on the total power of the network nodes.

The disadvantages of Proof-of-Work are obvious. A huge amount of processing power is wasted on performing useless calculations. The validity of the algorithm is also very controversial. Roughly speaking, it boils down to the simple rule, “Whoever has more powerful equipment is right.” In other words, success entirely depends on the amount of money invested in the equipment. Not to mention the energy costs and associated environmental problems, and the emergence of a whole industry of specialized devices like ASICs, which are absolutely useless for anything other than solving problems in the blockchain of a particular cryptocurrency. In addition, a large player can take control of the network by gaining 51% of the total computing power.

Another fundamental flaw associated with the given algorithm is the layout of the architecture itself, which can be used for centralizing the network. The ever-increasing complexity of the task of finding consensus requires increasing the costs of computing power. If the network is relatively small, there are enough resources on a home computer. But as it develops, the associated equipment costs constantly increase. This leads to the unification of network participants in order to increase the chances of adding a block to achieve uninterrupted rewards and stable paybacks and earnings, which has led to the appearance of mining pools. However, this has the potential of placing the network under the control of large players.

It is fundamentally important to note that each member of the network receives a reward for their work. The remuneration is paid for a successfully added block and, as a rule, consists of two parts:

- The commissions from the total amount of transactions included in the block. Some will realize the ability to set a higher commission for their transaction so that miners have an incentive to add the transaction to the block they form.

- A fixed block reward for mining. A fixed block reward may decrease over time. For example, this is how Bitcoin halving works.

In PZM Cash, the developers abandoned the delegated Proof-of-Stake and applied a significantly improved “classic” PoS algorithm. This has given a broad range of users the opportunity of participating in the network and receiving remunerations, as there are no significant restrictions or any substantial barriers.

The PZM Cash PoS Consensus Algorithm

The PoS consensus algorithm implies that the probability of a participant adding a new block depends on the size of their stake – the number of coins on the balance of their wallet on the network. The more coins on the balance, the higher the chance.

To add a block, it is also necessary to solve a problem (similar to PoW), however, the complexity of this task is determined individually for each user. The more coins on the wallet, the simpler the calculation.

Classic PoS involves the distribution of all coins at once between users and the use of transaction fees as a reward for network maintenance at the launch of the network and the formation of a genesis block. There are models where the amount of payment for adding a block depends on the indicator of the age of the coin, which is the result of multiplying the total number of coins by the duration of their storage by each user. This provides an incentive for users to keep the coins on their wallets and guarantees their shortage in circulation.

PoS is also subject to centralization, but buying coins is much easier than buying equipment and setting up mining, as in PoW, which provides an internal mechanism that restrains monopolization due to the large number of coin purchasers and owners.

The main advantage of the Proof-of-Stake algorithm, and the main reason for its development, is the guaranteed protection against 51% attacks. To carry out an attack, users need to buy up 51% of the total current amount of coins available. In fact, one user must buy a “controlling stake”, which is unlikely. In addition, since in the case of a 51% attack most of the coins will be on the balance of the initiator of the attack, the main victim of such an attack will inevitably be the attacker. This makes the attack not only extremely difficult, but also completely meaningless.

The main postulates of the PZM Cash PoS:

1. The chances of adding a new block depend on the number of coins on the account, or the forging balance;
2. The age of the coin does not affect the amount of the reward for adding a block;
3. The forging balance consists of user-accessible coins that are static on the wallet for a certain period of time and coins that were not involved in transactions, including unconfirmed ones;
4. The amount of the commission fee is 0.5% of the amount of transactions and is fixed. The participant who added the block is paid 0.5% of the total amount of all transactions included in the block;
5. No other payments are provided.

The Process of Adding Blocks

The process of adding a new block is associated with the main network process – the conduct of transactions and it starts on the user side. To describe the operation of PZM Cash, we must clearly limit the processes of the user and the kernel. Transactions have nothing to do with the kernel, as they are initiated on the user side.

The user enters their wallet address with the private key and creates a transaction. The process is as follows:

1. The user indicates the parameters of the transaction, such as the amount, the public key (address) of the recipient, etc. Users can create a transaction only after correctly filling in all its parameters in the wallet. The public key (address) of the person or contract to which PZM Cash is sent is also required.

2. A request for a transaction is generated. The software that connects to the cryptocurrency network informs the network of its intention to conduct a transaction. The easiest option is to use the lightweight PZM Cash cryptocurrency wallet.
3. Active nodes in the cryptocurrency network double-check the history of the blockchain and make sure that there really are coins on the user’s balance that the user intends to send.
4. After confirming the possibility of a transaction, the transaction is signed by the private key and sent to the pool of unallocated transactions that are waiting to be added to the blockchain. It is from this pool that forgers collect transactions into the blocks they are trying to add.
5. Next, the transaction should fall into the block. Subsequently, nodes on the network will also need to double-check it. The transaction cannot be canceled or changed after confirmation. Users can only start a new transaction.

The transaction should be recorded on the blockchain. This process takes place on the kernel side, which also includes the consensus algorithm. The kernel does not operate with individual transactions, but with blocks, in which the transaction is just one of the records. The blocks are a product of the consensus algorithm, and they determine in what order the transactions will be included in the transaction log and in which order they are conducted.

The next step is to decide who will form the next block in the ledger.

Who has the right to add a block?

As already noted, a local copy of the blockchain is stored on each node on the PZM Cash network. Each account that is not blocked by the publication of the private key of this account has the ability to generate blocks, provided that at least one incoming transaction in the account was confirmed 1,440 times. Any account that meets these criteria is eligible for forging.

How is a block generator selected?

To participate in the process of forging a block, an approved account signs the previous generated block with its public key. The signature is then hashed using the SHA256 hash function.

The uniqueness of the PZM Cash consensus algorithm is related to the calculation mechanism, which has some similarities with the Proof-of-Work algorithm.

Under PoW, all miners participate in a sort of competition to find the hash of the required type with a certain number of zeros at the beginning of the hash record. The desired value can only be obtained by enumerating the values. At the same time, the number of zeros at the beginning of the required record gradually grows, thus the number of options that need to be sorted out, and the required power to add a block at the required time, grows as well.

In PZM Cash, the search for the required hash is arranged in a similar way, however, the calculations do not become more complicated, but simplify over time, as the number of values matching the criteria gradually grows. It is the level of complexity of calculating the hash of the next block that determines the probability of generating a block. The more complicated the calculation, the lower the probability. Moreover, the complexity for each specific forger is different.

The basic rule is that the generator, which first receives the hash value below the set bar, gets the right to form a block. Over time, the bar increases, which guarantees the required speed of adding a block (to ensure the speed of the network), since the “permissible error” of the desired hash value is higher and the number of correct outcomes is greater.

In PoS, a participant with a large stake (coin balance) has a good chance of forming a block. The more coins in the wallet, the higher the “individual bar” and the chance of adding a block. In PZM Cash, the balance of the wallet, which was static on this account for 1440 blocks minus the coins involved in unconfirmed sent transactions is considered as the base factor. Each node turns to the wallet to request the balance and calculate the degree of increase for the bar.

As a result, the forger, which will receive the required hash value earlier than the others, below the bar set for it, gets the right to form a block and add it to the blockchain. Transactions in a block are collected from a pool of unallocated transactions. The maximum number of transactions for one block is 255. A record of transactions is made in the block that got there from the pool. Other data is also entered, for example, a hash, etc. The total number of transactions is limited by the block size. The generated block is sent for validation to the nodes, which confirm its correctness. Transactions are considered safe after 10 block confirmations. After the block has been correctly added, all transactions included in it are considered to be confirmed. The coins are redistributed and the commissions are paid. Confirmed transactions cannot be corrected or changed since they are permanently recorded on the blockchain.

Forging

The term forging is used as opposed to the term mining, which is characteristic of PoW. It means using minimal computing power to reach consensus, as opposed to Proof-of-Work.

The uniqueness of PZM Cash forging lies in the fact that it does not add any new coins to the network, since there is no reward for forging, which leads to the emergence of additional liquidity on the network. The only payment foreseen for forging is a transaction fee of 0.5% of the total amount of PZM Cash coins in transactions that were entered into the block.

Transactional fees are awarded to an account when it successfully creates a block. As the network expands, the number of transactions within it grows respectively, and earnings in the form of forging will increase.

Network settings

For ensuring the interactive display and affordable monitoring of the status of the PZM Cash network, the website has implemented the PZM Cash Explorer analytical interactive form, where each participant can see the network’s current performance, coin turnover and transaction fees.

On average, a new block is generated every 60 seconds. This logic does not depend on the number of transactions, however, the maximum number of transactions that a single block can contain is limited to 255. With maximum network performance – the maximum number of transactions per block – PZM Cash can confirm up to 367,200 transactions per day, or 1,440 blocks per day.

Security

- The time-tested SHA256 cryptographic hashing algorithm is used on the Merkle-Damgor structure.
- To carry out an attack of 51% and have the ability to exclude transactions or change the order of transactions, an attacker needs to gain control over 51% of all PZM Cash coins by gaining control of or bribing, coaxing forgers. This is highly unlikely with the increasing development of the network.
- An attacker can try to increase their likelihood of forging by shuffling or moving a large number of coins to one account. To avoid such actions, the rule of PZM Cash static is introduced in the account for 1440 blocks (24 hours). It is these coins on the balance that determine the probability of forging. In the event of such an attack, an attacker will not be able to forge anything during the day, which will result in big losses.

4. The Development Model

Our strategic goal is the rapid growth of the ecosystem. This is important because:

1. The emergence of new projects creates additional value for consumers by adding new products and services.
2. An increase in demand leads to a balancing of supply, and an increase in turnover contributes to the stability of PZM Cash in relation to the external environment, providing stability and strengthening of the exchange rate.

For successful development, it is necessary to provide a reasonable algorithm for ensuring the network with liquidity, or the emission of PZM Cash coins, as well as channels for scaling the network.

Participants in the PZM Cash public ecosystem may be:

- Private projects;
- Individual users;
- Developers and creators of projects and applications;
- Funding and investment providers (VC, angels, investors, accelerators, incubators);
- Public and state agents;
- Associations, unions and associations;
- Other participants.

Participation in the ecosystem provides a set of competitive advantages:

- Access to a growing and solvent client base that allows users to scale their business and increase profits.

- Technical and technological solutions and automation of business processes, such as a mutual settlements system, smart contracts system, the formation of a company’s work history, tracking the reputation of counterparties, countering falsification, etc.
- The ability to build partnerships and value chains.
- Improving business reputations and status as the environment develops.
- Access to financing and attention of venture funds and other sources of financing.
- Access to the international market when joining a network.

Network liquidity

It is obvious that supply and demand form the price of goods and services. It is the supply and demand for the currency that forms its exchange rate. The key issue of any cryptocurrency is the question of the stability of its exchange rate with respect to fiat money and other cryptocurrencies. In order for the rate to be stable, it is necessary to ensure a sufficient supply of PZM Cash coins, which is formed in the ecosystem according to the liquidity filling algorithm, as well as sufficient demand for the currency, which is ensured by an increase in the number of services available and use case scenarios for the participants.

Demand for PZM Cash will grow due to:

- The integration of partners that will use PZM Cash as a payment unit;
- dApps and Apps development (network expansion services).

On the other hand, we must provide the necessary mechanism for ensuring the network with liquidity and the emission of PZM Cash coins. Ecosystem liquidity in PZM Cash coins will be issued in two stages:

- Initial offering of PZM Cash (at the pre-mining stage);
- Expansion of PZM Cash liquidity (at the PoS mining stage).

The initial offering is the PZM Cash coins, which will be distributed during preliminary implementation (pre-mining) during the genesis of the first block. The initial offering is the amount of PZM Cash with which the network will start operating. That is, this is the starting liquidity for launching the system. Anyone who becomes a member of the network at this stage will receive an advantage due to early entry, because they will get the right to receive additional liquidity through PoS mining before the remaining participants.

With the launch of the main network, the process of expanding liquidity via PoS mining will be launched. The increase in liquidity in the PZM Cash ecosystem will occur due to the income received by the network participants for participating in it.

PoS mining is the only mechanism for additional emission of PZM Cash, no other mechanisms are provided. Forging, as a way of obtaining coins through the provision of network maintenance services, does not create additional liquidity, but represents a stream of redistribution of coins from transaction participants to participants registering these transactions. Redistribution flows do not increase the total number of PZM Cash in the system. They do not lead to an increase in liquidity in the network. These include:

- Transaction fees;
- Payments related to smart contracts;
- Payments for other operations;
- Exchange operations (PZM Cash - crypto, PZM Cash - fiat).

Pre-mining

The initial emission is 90 million PZM Cash, or 1% of the total final liquidity, which will amount to 9 billion PZM Cash).

The distribution of coins will be implemented as follows:

- 0.7% (63 million PZMC) allocated to the Public Sales;
- 0.1% (9 million PZMC) for the PZM Cash team with a one-year locup period;
- 0.2% (18 million PZMC) on marketing campaigns for three years after the launch of the blockchain;

- The coins will be issued and distributed and sent to the addresses of account owners with the launch of the network, which will start with the generation of the genesis block in the network;
- Upon initial issuance, the coins will be distributed in a decentralized fashion among a large number of participants, which will make up the initial user base;
- According to PoS logic, initial users will receive the benefits of early entry, which will allow them to start forging ahead of the rest.

PoS mining

PoS mining is provided as the only mechanism for increasing the liquidity of the network and is a mechanism for providing balance increase to loyal users of PZM Cash. It provides for the accrual of PZM Cash at the rate of accumulation on the balance on any activated wallet of the participant. In this case, only the current wallet balance is taken into account, which does not include coins entered into unconfirmed transactions.

The rate of increase is expressed in monthly percentage terms and depends on two parameters:

1. The current balance on the active leading wallet.
2. The current total balance on supporting wallets, or the wallets that have been added by the owner of the leading wallet as supporting wallets.

Forging rates do not change over time. To avoid dangerous centralization of the network, the maximum balance of one wallet can be 1,000,000 PZM Cash (or 0,011% of the total final liquidity, which will amount to 9 billion PZM Cash). Upon reaching this balance value, PoS mining for this wallet becomes unavailable.

How is the supporting wallet activated?

As mentioned earlier, a wallet is activated by an incoming transaction to this wallet using a public key. It is important who the transaction came from. The wallet is activated by the sender, or the leading wallet, as it introduces a new user to the network. Thus, the wallet activated by the transaction becomes the supporting wallet. In this case, the newly activated wallet receives the rights of the leading wallet. Therefore, each leading wallet has a unique supporting wallet structure.

PoS mining becomes available for the wallet from the moment it is activated. To do this, the leading wallet must list at least 1 PZM Cash in the incoming transaction.

How is the coins increase rate calculated?

The coin increase rate is the usual rate of accrual for a percentage calculated on a two-factor basis. The build-up rate is the base rate of return and depends on the current wallet balance. The multiplier depends on the number of coins on the supporting wallets for each particular leading wallet. Both values become higher as the total number of coins increases. Supporting wallets are structured to a maximum depth of 2 levels.

Table 1

Metrics for calculating the coins increase rate

Leading wallet balance	Monthly rate	Sum of supporting wallet balances	Multiplier	Multiplier Order (min and max values) in % per month
Top holders		Full network		
700,000 – 1,000,000	6,89%	More than 100,000,000	3,14	21%
500,000 – 699,999	5,35%	30,000,000 – 99,999,999	3,0	
300,000 – 499,999	4,14%	10,000,000 – 29,999,999	2,9	
Simple holders		Full network		
200,000 – 299,999	3,69%	5,000,000 – 9,999,999	2,7	
100,000 - 199,999	3,15%	1,000,000 – 4,999,999	2,5	
50,000 – 99,999	2,63%	500,000 - 999,999	2,3	
20,000 – 49,999	2,11%	200,000 – 499,999	2,1	
Minority holders		Starting network		
10,000 - 19,999	1,70%	100,000 - 199,999	1,7	
5,000 - 9,999	1,61%	50,000 - 99,999	1,6	
2,000 - 4,999	1,52%	20,000 - 49,999	1,5	
1,000 - 1,999	1,43%	10,000 - 19,999	1,4	
500 - 999	1,37%	5,000 - 9,999	1,3	
100 - 499	1,28%	1,000 - 4,999	1,2	
1 - 100	1,20%	Less than 1,000	1,16	
		0	0	1,20%

The calculation is made according to the value of the effective rate, which is calculated by multiplying the rate of increase by the multiplier. The maximum rate of coin increase for a participant is 21% per month, the minimum is 1.2% per month or 14.4% per year.

When are the additional coins paid?

The accrued coins are credited upon confirmation of any outgoing wallet transaction or change in current balance. At this moment, a “cast” of the balance of the supporting wallets is made. The coins that are in the pool of unallocated transactions and are awaiting sending are not included. Thus, the more outgoing transactions are made from the account, the more often payments are made. On the other hand, it also makes economic sense to keep coins on a user’s wallet and receive accruals according to the compound interest scheme.

5. Network scaling

As already noted, the main characteristic of PZM Cash is its orientation to the rapid scalability of both the money supply and the offer of services from developers and partners. The development and scaling of the PZM Cash infrastructure can be carried out in several directions.

1. Creating dApps

In this case, any developer can deploy their decentralized application. They will thus be allocated their own sidechain recorded on top of the main ledger. In this case, each user of the application will have their own wallet.

2. Export protocol

The source code of PZM Cash is open to everyone, which allows any developer to implement the PZM Cash protocol in their project as a kernel. To do this, users must deploy and run the full network node and install and synchronize a special API module.

3. Currency at partners

PZM Cash can be used as a means of payment on partner projects and platforms. The Web 3js technology implemented in the PZM Cash Wallet allows users to use the wallet to make payments on partner platforms, such as exchangers, exchanges, IM, etc.

6. Project Roadmap

Q2 of 2020

- Public sale of PZM Cash;
- Launch of the main PZM Cash network and online wallet;
- Listing on CoinMarketCap.

Q3 of 2020

- Launch of Android / iOS Wallets;
- Launch of Web3js;
- Creation of a network of exchange points;
- Entry onto the Asian markets;
- Active involvement of application and service developers.

Q4 of 2020

- Launch of the ability to create smart contracts;
- Entry onto the Latin American market.

Q1 of 2021

- Creation of an ATM network and issuing debit cards;
- Opening of PZM Cash Foundation technology hub.

Q2 of 2021

- The first international PZM Cash Summit conference.

Q3 of 2021

- Integration of new partners and services to expand payment methods.

7. CAUTIONARY NOTE ON FORWARD-LOOKING STATEMENTS

All statements contained in the given White Paper, statements made in press releases or in any place accessible by the public and oral statements that may be made by PZM CASH or their respective directors, executive officers or employees acting on behalf of PZM CASH (as the case may be), that are not statements of historical fact, constitute “forward- looking statements”. Some of these statements can be identified by forward-looking terms such as “aim”, “target”, “anticipate”, “believe”, “could”, “estimate”, “expect”, “if”, “intend”, “may”, “plan”, “possible”, “probable”, “project”, “should”, “would”, “will” or other similar terms. However, these terms are not the exclusive means of identifying forward-looking statements. All statements regarding PZM CASH’s financial position, business strategies, plans and prospects and the future prospects of the industry which PZM CASH is in are forward-looking statements. These forward-looking statements, including but not limited to statements as to PZM CASH’s revenue and profitability, prospects, future plans, other expected industry trends and other matters discussed in this White Paper regarding PZM CASH are matters that are not historic facts, but only predictions.

These forward-looking statements involve known and unknown risks, uncertainties and other factors that may cause the actual future results, performance or achievements of PZM CASH to be materially different from any future results, performance or achievements expected, expressed or implied by such forward-looking statements. These factors include, amongst others:

(a) changes in political, social, economic and stock or cryptocurrency market conditions, and the regulatory environment in the countries in which PZM CASH conducts its respective businesses and operations;
(b) the risk that PZM CASH may be unable or execute or implement their respective business strategies and future plans;
(c) changes in interest rates and exchange rates of fiat currencies and cryptocurrencies;
(d) changes in the anticipated growth strategies and expected internal growth of PZM CASH;
(e) changes in the availability and fees payable to PZM CASH in connection with their respective businesses and operations;

(f) changes in the availability and salaries of employees who are required by PZM CASH to operate their respective businesses and operations;

(g) changes in preferences of clients of PZM CASH;

(h) changes in competitive conditions under which PZM CASH operate, and the ability of PZM CASH to compete under such conditions;

(i) changes in the future capital needs of PZM CASH and the availability of financing and capital to fund such needs;

(j) war or acts of international or domestic terrorism;

(k) occurrences of catastrophic events, natural disasters and acts of God that affect the businesses and/or operations of PZM CASH;

(l) other factors beyond the control of PZM CASH;

(m) any risk and uncertainties associated with PZM CASH and their businesses and operations, the XXX Tokens, the PZM CASH Initial Token Sale and the PZM CASH Wallet (each as referred to in the White Paper).

All forward-looking statements made by or attributable to PZM CASH or persons acting on behalf of PZM CASH are expressly qualified in their entirety by such factors. Given that risks and uncertainties that may cause the actual future results, performance or achievements of PZM CASH to be materially different from that expected, expressed or implied by the forward-looking statements in this White Paper, undue reliance must not be placed on these statements. These forward-looking statements are applicable only as of the date of this White Paper.

Neither PZM CASH nor any other person represents, warrants and/or undertakes that the actual future results, performance or achievements of PZM CASH will be as discussed in those forward-looking statements. The actual results, performance or achievements of PZM CASH may differ materially from those anticipated in these forward- looking statements.