VESTCHAIN

WHITE PAPER

BLOCKCHAIN SOLUTIONS FOR BUSINESS

1. Introduction

VESTCHAIN is a global technology company building private and public blockchain solutions on a secure, flexible, and scalable blockchain solution. The platform is business-oriented, ensuring the security and scalability that business networks require in order to take full advantage of blockchain-based decentralized systems. Our network comes with three core features: 1) a closed ecosystem; 2) decentralization; 3) transparency. The network is capable of processing up to 1 million transactions per second, allowing businesses and other organizations to take advantage of the blockchain technology on a new scale.

2. Motivation

Data sharing has become a major driver of the economy. The speed, scalability, governance, and costs at which companies share data with stakeholders are significantly limited by the existing centralized systems. More so, a blockchain network can address conflicts between a company and stakeholders by executing pre-agreed smart contracts or by fixed documentation collection and automated verification. Blockchain-based decentralized networks can bring business data sharing to a new level at lower costs, provided they are adequately implemented.

In terms of implementation, transaction speeds are without a doubt one of the main barriers that limit cryptocurrencies' capacity of penetrating new markets. For instance, Bitcoin can only process around 3-7 transactions per second (TPS) while Ethereum can process 7-15 TPS.[1] Visa, on the other hand, can process 24, 000 transactions per second.[2]

VESTCHAIN provides blockchain solutions on a decentralized blockchain capable of processing faster transactions for free. The cryptographic component of the network will allow creating smart contracts and developers will be able to develop decentralized applications (dApps) independently. In other words, the network is meant to function as an operating system with a friendly interface.

With VESTCHAIN, users will be able to process a number of operations that in the peak time will reach about 1 million per second thanks to a design based on Delegated Proof of Stake (DPoS).

1 https://github.com/ethereum/wiki/wiki/Sharding-FAQ#this-sounds-like-theres-some-kind-of-scalability-trilemma-at-play-what-is-this-trilemma-and-can-we-break-through-it

2 Wang, Y., Yang, J., Li, T., Zhu, F., & Zhou, X. (2018, July). Anti-Dust: A Method for Identifying and Preventing Blockchain's Dust Attacks. In *2018 International Conference on Information Systems and Computer Aided Education (ICISCAE)* (pp. 274-280). IEEE.

3. A New Business Paradigm: Blockchain-Based Distributed Networks

3.1. Vision

The complex structures and operations that characterize any major business are difficult to manage on a centralized system. At the present time, blockchain companies have rarely focused on B2B solutions, despite the many advantages that decentralized decision-making can bring. We strongly believe that in the near future operations taking place in areas such as the automotive industry, logistics and retail will operate on a decentralized system.

The blockchain technology gives owners full control over their data, including the authority to choose whether to share their data and with whom. In a world where data privacy is a growing concern, many businesses may perceive features such as decentralization of information and full ownership over their data and more desirable than ever. VESTCHAIN believes that the blockchain is the future of data sharing and seeks to build a trust-free business environment that can accommodate a variety of business types of activities.

We seek to make cooperation between business entities simple and efficient, allowing businesses to focus on their products and services. This goal is achieved through several features included in the environment.

One such feature is allowing businesses and individuals to obtain fair rewards based on their contribution. We find it equally important to create a working environment that allows for a lower trust cost between the interacting parties. Last but not least, we seek to create an infrastructure where individuals, businesses, and communities can connect with each other safely and efficiently to exchange products and services.

3.2. Who Can Participate?

VESTCHAIN can provide services for several types of participants, including:

- Business owners: Individuals, private companies, non-profit organizations, and governmental entities, among others, can use VESTCHAIN to provide a significant variety of products and services. A functional distributed business environment will require the active participation of all the members in the community.

- Smart Contract Providers: Participants can create smart contracts and provide them to others in exchange for coins, goods, or services

- Infrastructure Providers: Users can protect the VESTCHAIN ecosystem through block generation and verification.

3.3. Data Sharing on Decentralized Networks

Many businesses have difficulties in handling increasing data sharing demands. Traditional centralized systems are not designed to manage the velocity of interactions demanded by current data needs, which forces companies to spend significant resources in connecting systems, processing and verifying data, as well as paying those who can perform these services for them.

Companies can benefit significantly from business-focused blockchain platforms that are designed to deploy distributed business networks. Core features of the blockchain, such as decentralization and disintermediation, can assist organizations in connecting with each other faster while engaging less human and financial resources.

3.4. Integrating Internet of Things (IoT) and the Blockchain

The concept of IoT was proposed in the late 1990s by Kevin Ashton and can be described as a network including all smart devices where they communicate with each other on the cloud without the need of human interaction. [3]Until recently, the development of IoT was relatively slow due to small connection capacity, limited coverage area, and high costs, among others. While IoT has improved in these areas in the last couple of years, it still suffers from some major limitations that can be addressed by the blockchain technology, including high development and maintenance cost, fragmentation of the standard communication protocol, and lack of privacy.

We believe that the blockchain can make IoT significantly more powerful than it is today, effectively transforming many industries. For example, IoT can be used to perform automatic transactions through the use of smart contracts. More so, IoT-blockchain can be combined with artificial intelligence (AI) and big data for an even stronger impact. [4]

Perhaps the most important addition that the blockchain can provide to IoT is enhanced security. As in the case of other applications, the centralized paradigm under which IoT applications currently function (centralized clouds) makes them more vulnerable to attacks. The only known point of vulnerability that an

3 Kramp, T., Van Kranenburg, R. and Lange, S., 2013. Introduction to the Internet of Things. In Enabling Things to Talk (pp. 1-10). Springer, Berlin, Heidelberg.

4 Kshetri, N., 2017. Can blockchain strengthen the internet of things?. IT professional, 19(4), pp.68-72.

IoT application working on the blockchain will have is the click needed for time stamping.[5]

An area where the blockchain can certainly provide additional security is supply chain. For instance, blockchain-based applications can make handling and managing crisis situations such as product recalls due to security problems easier. Because the blockchain is publicly available, it is always possible to trace back every product to the origin of the raw materials and, as such, transactions can be linked to detect users of vulnerable IoT devices.[6]

Blockchain-based applications can improve complex workflows that take place in supply chains. For instance, such applications can be used to register the location, price, time, and other information when the ownership of an item changes. More so, the blockchain can track raw materials as they move through the chain, are transformed, integrated, and sold. Finally, the blockchain can be used to register updates, patches, and part replacements applied to any product throughout its lifetime, making it easier to track progress, address vulnerabilities, and send warnings.

The blockchain technology is ideal to integrate different elements of IoT, as it provides a logical language that can be used by applications to communicate irrespectively of where the equipment on which they are based was built.

The VESTCHAIN platform includes all the components required for IoT elements to communicate on the blockhain, namely personal identification and smart contracts. Personal identification can allow manufacturers to communicate with each other without fearing someone can manipulate the identification code (which is not controlled by anyone) while smart contracts ensure that the transactions are secure and transparent.

3.5. Key Features of Distributed Business Networks

Three important features of a distributed business network are 1) the use of blockchain clouds that eliminate businesses' need to invest in IT infrastructure; 2) data is protected through proven mechanisms; and 3) well-designed distributed networks comply with regulatory standards that offer the needed legal protection.

Each community (e.g., company, governmental agency) can operate on its own cloud-a system wh4ich organizes hardware, software, and liability nodes

5 Kshetri, N., 2017. Can blockchain strengthen the internet of things?.
6 Kshetri, N., 2017. Can blockchain strengthen the internet of things?.

through the protocols set on the globular network that allows for peer-to-peer coordination. Domains within a cloud can be used to set procedures for business services for long-term trading for storage, traffic, and CPU. More specifically, organizations can connect with each other through delegation (discussed in the next section) at faster speeds compared to traditional networks without the need to rely on their own IT infrastructure but relying instead on blockchain clouds.

OmniScaling allows utilizing several nodes, storage chains by combining deterministic role allocation, individual validation groups per transaction, and network membership. This approach allows for dynamic scalability by storage capacity, traffic, and CPU. Per-transaction consensus allows the requirements to be set as a business logic component to match the value and risk of the transaction versus the cost and speed of validation.

Data safety is made possible through permissioned node access, atomic re-encryption, signatures from nodes that have accessed data, and data scattering. Data scattering can significantly reduce the impact of data leakage and intrusions for off-premise configurations.

In order to ensure compliance, businesses can document anything they want to legally binding signatures of those who have participated in operations as well as details concerning the place, date, and procedures describing those operations.

Through the use of a distributed business network, VESTCHAIN can help clients from any part of the world take advantage of a cloud architecture based on the blockchain technology that can solve real business needs at reduced costs and higher revenues compared to traditional business services. With VESTCHAIN, individuals and companies can explore new revenue sources that were not accessible through traditional channels, such as business models based on digital assets and supply chain of information.

VESTCHAIN seeks to digitalize and connect the core elements of any business process: individuals, objects, and assets. Business processes are coordinated through smart contracts-the fundamental feature of our network used to create a distributed business environment that is trust-free a decentralized. In other words, the platform can be used to digitalize business activities and participants, reducing the cost of industries and improving business efficiency by optimizing the distribution of resources.

With smart contracts, users can:

- Establish relationships with different object data
- Provide authorizations for customization and modeling
- Communicate and merge with different business models
- Develop an interconnected distributed business model.

3.6. The VEST Token

VESTCHAIN provides services and resources in exchange for VEST token-an utility token that works on a DPoS algorithm. Each domain will connect to other domains based on contracts that provide the available services. A business gets its own network identity through which it can share and access data with others. Through a domain, users can operate on different governance models and create policies for their data.

We provide provides support for large transactions, allowing building business services to become significantly less difficult with a system that reduces the resources required to develop and deploy the storage and processing of off-chain documents.

3.7. Addressing Specific Scenarios on Each Operation Layer

There are several scenarios in which participants can operate on the VESTCHAIN platform. These include business customers who are running their own business service on the platform, businesses who are represented within the platform but don't have any services, cloud operators charged with managing financial and legal liability between participants, hardware capacity providers, and vendors who provide business service templates for the platform. Business templates make possible the reuse of business logic as application templates or components.

Different participants operate on different layers and have unique needs that the platform seeks to address. These needs include ready-to-deploy business solutions, blocks for applications and services, toolkits to access platform execution layers and integration or external functions, scalability and rebalancing mechanisms, sharding and execution tracing, and node connectivity and security.

3.8. Technological Development

VESTCHAIN will continue its technological development by focusing on three core elements that characterize most development plans: R&D, development, and testing. Investing resources in R&D is fundamental in order to ensure that VESTCHAIN will continue to improve its technology by upgrading the existing features of the platform or by creating new ones. Feasibility analysis for all developmental paths considered is a key component of the R&D that takes place at VESTCHAIN.

During the development phase, new products or services are tested. Products or services that fail to meet expectations are either improved or rejected. In most cases, given the human and financial resources dedicated to R&D, we will prefer to invest additional resources to improve the products that failed initial testing.

The last phase includes re-testing the products after it has been improved following the initial test results (if it applies). Deployment and maintenance efforts also take place within this last phase of development and they are focused on detecting problems early on in order to ensure high satisfaction with the products and mitigate costs.

3.9. Market Opportunities

The governance structure provided by VESTCHAIN will prove to be particularly useful to industries that rely on supply chain record keeping, which include the automobile, medicine, and cold-chain logistics industries, among others. The distributed ledger technology ensures that the information exchanged on the platform is accurate and secured during all steps of a transaction. As such, the buying process will be faster, as buyers won't need to spend time searching for fake or hidden information; everything will be securely stored on the blockchain.

The global cold chain market size is valued at over $167.99 billion and is expected to grow at 15.1% CAGR from 2018 to 2025. This strong market can benefit from IoT devices that ensure enhanced shipment safety by tracking specific metrics. Such devices can be connected to the VESTCHAN network, which will provide transparent information sharing through its distributed ledger technology.

Another potential market is the automotive industry, which is gradually incorporating IoT technology in order to improve record keeping. It is estimated that over 20% of cars will be released on the market with an IoT solution by 2020. The VESTCHAIN network can be used to store car data, making record keeping easier to manage.

Participants in the fashion industry are also potential clients of VESTCHAIN, as our platform can provide services for product management, production channels, and can help brands connect with their customers. For example, IoT products used on clothing products can function on the VESTCHAIN platform, allowing the recording of all logistic operations. Through these recordings, the customers can check the history of the product and, as such, verify its authenticity, something which is often difficult and time consuming through traditional means.

4. Core Concepts

4.1. Usability

Developers can face significant difficulties in inserting specific basic functions in a smart contract such as an account recovery and task scheduling. This is especially the case for users who lack a solid understanding of the basics of cryptography. By using an operating system protocol, VESTCHAIN will provide all the basic functions needed to create contracts, allowing developers to develop their projects without concerning themselves with cryptography.

Users can expect high TPS through the use of DPoS, where each block can store a virtual unlimited number of operations. As blocks are made of a multi-layer cell it can pack an entire operation into a compressed form after the final filling of the main block.

4.2. DPoS & Scalability

DPoS is a consensus mechanism that has been developed with the hope it will improve the blockchain in terms of democratization, decentralization, and transaction speed without sacrificing security. On this mechanism, token holders vote in delegates to validate transactions on their behalf. The number of voted delegates change periodically and range from 10 to 100. The framework allows voting out delegates that do not perform well or harm the system. DPoS is a collaborative system where delegates work together and operate faster than other existing systems, which makes it an attractive approach for any network aiming at addressing the scalability problem. Allowing delegates to establish direct connections before and after other delegates in the chain ensures that payment will be received and new blocks can be produced in an interval of 10-30 second. [7]

7 https://github.com/bitshares/bitshares.github.io/blob/master/_drafts/v1/2014-04-03-delegated-proof-of-stake.md

In the DPoS algorithm, all producers participate in the generation of blocks and a transaction confirmation occurs within 2 second after sending. In the event of a system failure, the network requests confirmation from 40 out of 50 producers which takes no more than 60 seconds. In such a case, the problem block is marked as mandatory. In the case of forking, producers are switched to a chain with presence of obligatory blocks.

DPoS blockchains do not have typical forks; the producers of the blocks cooperate as opposed to competing with each other. When forks occur, the system switches to the longest chain of blocks. A chain with many producers grows in length faster, which makes it easier to determine the fork attempt. Produces who will try to create forks will be excluded forever.

DPoS has some advantages compared to PoW and PoS that are to be taken into consideration. For instance, DPoS provides incentives to nodes that act honestly, which reduces the risk and increases scalability. With PoW, someone could create a hard fork if they gained the majority power in a network, reducing the security concerns associated with having groups of miners separated. With DPoS, an actor can lose its power through a democratic voting process, as the system does not rely on the processing power of a few, which suggest the system may be more decentralized. In typical network conditions, chain forks are unlikely to occur and can be solved in a few minutes.

With VESTCHAIN, blocks are generated every 5 second in stages of 50 blocks. In the first stage, unique producers for each block are selected by voting and a schedule is created. Producers have the right to create a block in order of a turn and when a producer does not fulfill the generation of blocks within 24 hours, the system excludes it until receiving a message of readiness to resume work. This approach allows for achieving continuous network operation.

4.3. Solving Scalability with Sharding

The scalability trilemma assumes that a blockchain system can only have two of these three properties: decentralization, scalability, and security. The lack of scalability can significantly limit the value of cryptocurrencies and other assets based on the blockchain on the long-run, as slow transaction speeds limit the ability of trading blockchain tokens for goods and services at a large scale. Addressing the scalability issues could enable blockchain systems to become a viable alternative to many traditional systems such as currencies, securities, and centralized applications.

Sharding is a Layer 1 solution to scalability. Sharding consists of separating the core network of a blockchain into several smaller parts (shards) to enhance the electronic voting machine (EVM) speed. Each shard behaves as its own blockchain and verifies each transaction through random miners. If the transaction is verified, the reference of the state of the shard is then stored on the main blockchain. Shards do not only communicate with the main chain but also with each other. Because nodes only need to synch the assign shard, they require less storage. Shares are not only be in communication with the main chain but also with one another[8].

VESTCHAIN operates on a two-level network. The first level consists of flexible segment blockchains (shards) and the second level consists of a core blockchain that validates all the blocks from the shard blockchain. Shards demand the same account and one wallet can be used for all the cryptocurrencies included in the shards.

We developed a base for stimulations which centers on a game theory; hash powers in it are encouraged to be shared among shards equally. 60% of all the hash power is assigned to the core chain to avoid episodes of double spending.

Individuals can engage in inter-segmental operations whenever they want, as approval is almost instant. The inter-segmental operation capacity is meant to grow linearly as the number of shards grows.

As TPS grows, the super-full node price is likely to rise as well, including to very high levels. With this in mind, the VESTCHAIN network is organized into numerous reliable nodes which together assume the role of a super-full node.

5. DApps Through VESTCHAIN

Any service or good can be decentralized and tokenized on the blockchain. DApps can be used for financial applications (including currencies and derivatives), governance applications, token systems, decentralized file storage, identity and reputation systems, and decentralized autonomous organizations.

There are currently over two thousand dApps operating on different blockchains. The number is likely to increase significantly in the near future, especially if the speed at which transactions can take place increases as well. For example, DApps will likely be an attractive option for companies that need to process from 50 to

8 Knirsch, F., Unterweger, A., & Engel, D. (2019). Implementing a blockchain from scratch: why, how, and what we learned. EURASIP Journal on Information Security, 2019(1), 2.

100 thousand transactions per second in a safe environment. Potential clients for VESTCHAIN includes financial institutions, large enterprises, technological companies, and social networks.

As the VESTCHAIN operates on a network that provides a higher transaction processing speed compared to existing networks, the number of dApps solutions requested could significantly exceed its predecessors.

6. User Accounts

Users can create accounts that they can easily remember, being able to choose any unique user name that is between 3 and 64 characters. Accounts are replenished with a small amount of money to add a record to the database. Account users can interact with each other through messages and process incoming message automatically.

When a database is created, new account users receive an encryption key. It is worth noticing that account users will be able to partially or fully delegate access to their database, which will allow them to take advantages of the benefits of joint management for different business operations. More so, users will be able to split management functions for a contract between users and, as such, determine to which cells of the database others will have access and what operations will be able to perform.

6.1. Conditions for Adding New Users (CAU)

Adding new users is performed in the same way as in the previous example, namely:

CAU = ESUn * ESUn

CAU = ESUn + ESUn

6.2. User Delete Condition (UDC)

If the consent of the person is required to perform the action, and this consent cannot be obtained due to unforeseen circumstances, a procedure for deletion from the system is performed without the loss of personal rights. More so, the removal procedure can be applied to participants in the organization that hinders its activity.

T - Time of user's absence on the network (in days) [optional]

ESUn-users - users whose signatures are required for confirmation (the signature of

the deleted user is not considered during the voting)

UDC = T + ESUn-users

7. Operations

7.1. Decentralized Organizations (DAO)

The client's platform allows creators to configure settings and invite new users. The authorized capital of DAO consists of funds provided by users and the transfer is carried out according to the principle: User-DAO. When users do not reach agreements within a specified time from the moment of the first payment funds are returned to the sender.

The system is based on pre-established requirements that must be fulfilled in order to perform a specific action. For each action, a set of variables have been developed that users can apply to create and configure the rules of the game. Starting a game consists of 1) defining the rules and 2) accepting the rules.

The organization management can be configured into rigid, flexible, and mixed management. Rigid management can be regarded as more bureaucratic yet providing a higher level of reliability and safety of assets by reducing the efficiency of decision-making. Flexible management is more

that are very active and need a system of consensus and conflict resolution between participants. Users who prefer a configuration that takes advantage of both forms of management can choose a mixed management configuration.

7.2. Facts and Indicators

Indicators contain the relation of one fact to another, and are expressed in the form [*] и [+]:

[*] – the logical multiplication of facts means that in order to perform an action, it is necessary to observe all facts.

[+] – the logical adding of facts, means that to perform an action it is necessary to observe at least one of the facts.

The fact is the consent of one or more users and is expressed by an electronic signature, functioning as a mechanism of rigid control. The designation of facts is referred to as an electronic signature of the user (ESU). Signatures can be simple or complex; simple signatures are single signatures and complex signatures are encompass two or more signatures.

Example:

1. ESU1 * ESU2 * ESU3 – the condition contains mandatory execution of 3 simple signatures

2. (ESU1 + ESU2) * (ESU3 * ESU4) – the condition contains mandatory execution of two multi-signatures. The second fact contains 2 mandatory signatures, and the first one presupposes the presence of one of the signatures.

7.3. Transaction Conditions (TC)

Creators of a system establish a list of persons whose consent is required for the transaction. Depending on the structure and objectives of the DAO, users can set out the condition for the transfer of funds.

The configuration of transaction conditions is divided into 3 types:

- Conditions for all transactions
- Conditions for transactions greater than N
- Conditions for transactions less than N

For example, let us consider a DAO with 5 users. The condition of the transaction in this organization is the signature of 3 users:

DAO; Balance = 100 VEST; Users = 5

TC = ESU1 * ESU2 * ESU3

In the following example, the transfer of funds requires the consent of one of the two users:

TC = ESU1 + ESU2

For complex hierarchical systems, the function of delineation of authority for transfers of funds is available. This means creating several parallel conditions for each transaction type:

TC > 100 VEST = ESU1 * ESU2

TC < 100 VEST = ESU1 + ESU2

To transfer funds in the amount of more than 100 VEST, 2 electronic signatures are required; to transfer funds of less than 100 VEST, one of the two signatures is required.

The number of conditions for each type of transaction has no limitations.

7.4. The Conditions for Establishing Ownership (CEO)

The ownership right allows users to reserve the share for the owner in the system. If the owner leaves the system or is excluded, the part of the funds equal to the users' share is blocked by the system and redirected to the personal wallet of the user or to the wallet successo. The released share remains in the ownership of the organization until its distribution. The right of ownership is expressed by the presence of voice tokens, which are displayed in the personal account of the user and reserve the ownership right for the organization.

Establishment of ownership rights is carried out at the stage of creating a system through the following expression:

CEO [100%] = (U1=50%) + (U2=50%) – User1 and User2 divided among themselves equal shares in the organization

The undistributed part remains in the ownership of the organization until it is distributed by its participants. To change the undistributed share, the condition is set.

This distribution of tokens can be revised, for example, when a user enters or leaves the DAO. For this purpose, a condition is created where, by agreement, users transfer votes to a smart contract, after which the smart contract distributes voice tokens between the participants in accordance to the specified shares.

Distribution of ownership (DO) = ESU1 * ESU2 * ESU3 * ESU4

7.5. Transfer of Ownership (TO)

The procedure for transferring ownership rights is established by the participants of the system. It can be open or closed.

In an open organization, a user can transfer/sell a share to persons who are not users of the organization. From the moment of obtaining rights, they become participants in the organization.

In a closed organization, transfer/sale is possible only among member participants. To transfer rights to a non-member, that person must first be added to the organization.

7.6. Change of Conditions (CO)

If a member wants to change the current condition, he enters the management section and initiates a change of the condition; the owner must choose the condition, create new requirements, and take it out to vote. The procedure for changing is determined when creating the DAO and two variables are set:

- The circle of persons who have the right to initiate a change = Users

- Required signatures for acceptance = ESUn

7.7. Consensus (Con)

Consensus is a flexible management tool that allows users to make quick decisions without waiting for the answer of all the participants of the organization. The mechanism is very simple and contains two variables:

- ESUn – electronic user signatures required to perform the action.

- Quorum – minimum number of signatures required to decide

Con = [ESUn] + [Quorum]

Consensus is possible for any action. The parameters of the consensus are set for specific actions by participants.

Example:

ESUn = ESU1 + … ESU20

Quorum = 11

In this example, the consensus consists of 20 people; for a decision to take place, 11 participants must give their signature. Users of DAO establish the following conditions:

Transaction Condition (TC)

TC > 1000 VEST = CON * ESU1

TC < 1000 VEST = CON

To make a transaction for less than 1000 VEST, we need to obtain consent in

the consensus, namely, the signature of 11 people. But for a transaction in the amount of more than 1000 VEST, one consensus is not enough, the signature of participant 1 is mandatory and without this signature consent the transaction will not be executed. In this way, you can set up any action, developing levers of management in the organization.

7.8. Internal Management of DAO

After setting up the conditions and creating an organization, its participants will receive a separate section within an organization in which the DAO management functions will be available. The actions will be carried out through a separate tab in the organization section, after which they will be put to an open vote and, if necessary, be confirmed by other participants. Once the condition of action is confirmed by facts (signatures of participants), the contract is automatically executed.

7.9. Right of Initiation

Users can receive the right to carry out internal and external management on behalf of DAO. For example, participants can make transfers on behalf of an organization by filling appropriate fields (address and amount) after which the proposed action goes into the control section and becomes visible to others. The action of the participant is displayed in the control section and, if necessary, awaits confirmation from the designated persons. This right applies to all possible management actions. If there is an intruder among the DAO participants, they cannot cause significant harm to the organization and others will be able to react quickly and delete the user from the participant list.

7.10. Right of Conservation

VEST titles allow allocating and maintaining a share in case of removal or withdrawal from DAO.

7.11. Inheritance Right

This right allows participants to specify the recipient of inheritance. In case a participant does not appear on the network for a certain time, all their property will be sent to a pre-established address. This will allow users to consider accidents and save their propertues. The right is configured as follows:

T (absence time in the network in days) = N

Heir = wallet successor

Any action taken in the DAO is recorded in its accounting book. Information about organizations and their actions is in the public domain. The accounting book contains data about the activities of the organization, namely:

- Information about the organization

- Balance

- Incoming and outgoing transactions

- List of participants in the organization

- Performed actions

- List of participants in voting and their decisions

7.12. Parallel Execution of Applications

VESTCHAIN confronts producers with the task of delivering messages to different threads. To implement this feature, the delayed message algorithm will be applied. In fact, a schedule will be drawn up for sending messages, and their delivery will be carried out at the next stage.

Sending and delivering messages from one user to another requires time. To minimize this, users should be given the opportunity to exchange messages within the block. For this, loops consisting of parallel threads are inputted into the block. Threads include transactions with messages whose delivery is scheduled for the next cycle.

Block

Cycles (successive)

Threads (parallel)

Transactions (successive)

Messages (successive)

Recipient and Notified Accounts (parallel)

Inside the block, there will be an analysis for the absence of threads that change the same account. The block producer can add cycles during the entire block generation period.

7.13. Assessment of the Blockchain State

As part of the network scaling, VESTCHAIN is divided into modules and individual network nodes can be customized. After a core is installed, a subset of applications can be selected for the node, for example, to organize an exchange or work with social networks. In this case, the node will only accept messages addressed to the selected applications.

The state of communication between users is transmitted through messages included in the blockchain, which means that one account cannot synchronously call another account, and attempts to substitute account information are excluded.

Block producers independently assess the complexity of the block, the time for confirmation of transactions, and automatic messages in smart contracts. Inside the network, all transactions have a fixed payment for bandwidth, but the block producer has the right to calculate the costs and decide whether a transaction consumes an excessive amount of resources. In this case, the manufacturer has the right to refuse to perform the transaction.

The refusal to perform the transaction will be confirmed only if all producers will consider the transaction as invalid. For any transaction, the producer can search for one minute. If the producer attempts to manipulate the block, a voting procedure will be initiated for his deletion.

7.14. The Token Model

Any blockchain has a resource base limitation and has the need for a security system. The main resource classes of VESTCHAIN includes the following:

- Bandwidth and Log Storage (Disk)

- Computation and Computational Backlog (CPU)

- State Storage (RAM)

The blockchain stores the history of all messages. Any of the network nodes must download and store a complete history for network synchronization, which makes it possible to restore the state of any application.

The computational backlog is used to deploy the blockchain state, that is, a list of calculations necessary to restore the network's history. When it becomes too large, state snapshots are performed and the past history is discarded. This parameter requires constant monitoring.

The state of the system consists of information received from applications about account balances and orders. Only those states that are read by the applications are stored. For example, if the application logic does not use post or comment content, the information will not be stored in the blockchain state; however, the existence of this post or comment, as well as other properties, will be saved.

7.15. Network Measurements

The resource toolkit is subjective, as producers of the blocks independently control and fulfill restrictions on the use of resources considering their algorithmic schemes. However, some things can be measured objectively, for example, the amount of data stored in the database or the number of messages can be measured quickly and cheaply.

7.16. Payment of Expenses

In traditional business settings, a company pays for office expenses, computing power, and more while the consumer receives the final product. The business expenses are covered by the income obtained from selling the product. A social network does not force users to pay for maintaining servers, offering instead paid services. Also, applications based on the blockchain should not oblige customers to bear the costs of using it. On the VESTCHAIN network, there is no payment for the use of the blockchain, which creates favorable conditions for the business to develop its own strategy for selling final products.

7.17. Delegating Capacity

The VEST token holder on the running software can lease the bandwidth for other network users. In this case, the producers of the blocks find such proposals and distribute the bandwidth to these nodes of the network, paying for the service with tokens.

7.18. Transaction costs and Token Value

Another advantage of the VESTCHAIN network is the complete independence of the bandwidth from the price of the token. To run a software based on VESTCHAIN, the owner must keep a certain number of tokens on their wallet. In this case, the application can run for an unlimited time within the bandwidth and state allocated for it.

Such a system ensures the independence of developers and users on VESTCHAIN from the costs of the tokens on the trading platform. The computing power, bandwidth, and storage space can be increased by augmenting the number of tokens in the account (shares in the network) and do not depend on the value of the token. Block producers receive a reward for creating a block. Due to the value of these tokens, the manufacturer can improve the system by purchasing new hardware.

7.19. Storage cost

On VESTCHAIN, the application developer must store tokens on the wallet in order to maintain the state of the application until this state is removed. If the application state cannot be deleted, the tokens will be eliminated.

Any account on the network must maintain a minimum balance on the wallet to store data on the network. Gradually, the minimum balance will be reduced.

7.20. Block reward

Block producers receive a reward for creating a block. To do this, a fixed number of tokens will be generated. Thus, the total annual release of tokens will always be constant and independent of external factors.

7.21. Community-friendly apps

Along with voting opportunities for the best block manufacturers, the community can select useful applications. Applications can be voted through a system of top-10 applications. In this system, voting will be conducted considering the number of tokens among users, meaning that the number of tokens is equivalent to the number of votes and each wallet token is equal to one vote. Thus, 10 applications that receive the majority of votes will receive additional compensation for a specified percentage of the total annual issue of tokens. This promotion will be valid as long as the application is in the top-10 by the number of votes.

An account owner can change their voting in favor of another app at any time. When top leaders change, the new contract starts receiving tokens from the next block.

7.22. Management

In this context, management refers to the process of solving issues related to the consensus-building that cannot be resolved algorithmically. The main source of power in the VESTCHAIN blockchain is the network token holder. More specifically, token holders transfer their power to the block producers and grant them limited and verifiable powers to freeze accounts, search for and fix defective applications, and submit fork proposals to the basic protocol.

The feature to designate block producers is embedded in the VESTCHAIN software. When making changes to the blockchain, block manufacturers must approve them. When a block producer refuses to fulfill the wish of the token holders, they may initiate a vote to eliminate the producer. If the block producer makes changes without the permission of the network users, the testifiers of the full nodes reject the change process.

7.23. Account freezing

In cases of unforeseen errors in smart contracts, violations of accounts, vulnerabilities found in account fragments, as well as excessive consumption of network resources, the block producer may decide to temporarily freeze their account until the problems are solved. The process initiated by one producer must be approved by the vast majority of producers.

When problems noticed by the producer are removed, the account will be frozen and the exchange of messages with the network will be resumed. In case of abuse of power, producers may be excluded, and the account will be frozen.

7.24. Updating the Protocol and the Constitution

VESTCHAIN initiates a process in which the following steps are required for the protocol:

- Block producers offer constitutional changes and receive 45/50 approval votes

- Block producers support 45/50 approvals during 30 consecutive days

- All users are required to sign transactions using a hash of a new constitution

- Block producers make the necessary changes to the source code to display the constitutional changes and offer them to the community using a hash of code changes

- Block producers support 45/50 approvals within a 30-day period

- Code changes take effect 7 days later, giving to all the complete nodes one week to update after the source code has been validated

- All nodes that do not switch to the new code are automatically disabled

The process of the blockchain updating and introducing new functions will take 2 to 3 months, and updates to correct minor errors without changing the constitution will take from 1 to 2 months

Contacts

Follow and contact us on social media: